Switch Software
Management and Configuration Guide

Abstract

This switch software guide is intended for network administrators and support personnel, and applies to the switch models listed on this page unless otherwise noted. This guide does not provide information about upgrading or replacing switch hardware. The information in this guide is subject to change without notice.

Applicable Products

HP Switch 3500 Series
HP Switch 3500yl Series
HP Switch 3800 Series
HP Switch 5406zl Series
HP Switch 5412zl Series
HP Switch 6200yl-24G (J8992A)
HP Switch 6600 Series
HP Switch 8206zl (J9475A)
HP Switch 8212zl (J8715A/B)

HP Part Number: 5998-4155
Published: February 2013
Edition: Software Version: K/KA.15.12

Acknowledgments

Warranty

For the software end user license agreement and the hardware limited warranty information for HP Networking products, visit www.hp.com/networking/support.

Contents

C Troubleshooting....388

1 Product Documentation

About your switch manual set

NOTE: For the latest version of all HP switch documentation, including Release Notes covering recently added features, please visit the HP Networking Web site at www.hp.com/Networking/support.

Printed publications

The *Read Me First* included with your switch provides software update information, product notes, and other information.The latest version is also available in PDF format on the HP website, as described in the Note at the top of this page.

Electronic publications

The latest version of each of the publications listed below is available in PDF format on the HP website, as described in the Note at the top of this page.

- *Installation and Getting Started Guide*—Explains how to prepare for and perform the physical installation and connect the switch to your network.
- *Management and Configuration Guide*—Describes how to configure, manage, and monitor basic switch operation.
- *Advanced Traffic Management Guide*—Explains how to configure traffic management features such as VLANs, MSTP, QoS, and Meshing.
- *Multicast and Routing Guid*e—Explains how to configure IGMP, PIM, IP routing, and VRRP features.
- *Access Security Guide*—Explains how to configure access security features and user authentication on the switch.
- *IPv6 Configuration Guide*—Describes the IPv6 protocol operations that are supported on the switch.
- *Command Line Interface Reference Guide*—Provides a comprehensive description of CLI commands, syntax, and operations.
- *Event Log Message Reference Guide*—Provides a comprehensive description of event log messages.
- *Release Notes*—Describe new features, fixes, and enhancements that become available between revisions of the main product guide.

2 Time Protocols

Command Summary

Table 1 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
no timesync	Disables time synchronization without changing the Timep or SNTP configuration	-	(page 42)	(page 24)
show sntp	Lists both the time synchronization method and the SNTP configuration	-	(page 45)	(page 36)
show management	Lists the IP addresses for all time servers configured on the switch, plus the IP addresses and default gateway for all VLANs configured on the switch	-	(page 24)	-
timesync sntp	Selects SNTP as the time synchronization method	-	(page 25)	(page 36)
sntp broadcast	Configures broadcast as the SNTP mode	disabled	(page 26)	(page 36)
sntp unicast	Configures unicast as the SNTP mode	-	(page 27)	(page 36)
[no] sntp server priority [1-3] *ip-address* [oobm] [version]	Enables, disables, and configures SNTP server in unicast mode	-	(page 28)	(page 36)
no sntp server	Deletes the specified SNTP server.	-	(page 28)	-
sntp poll-interval [30 - 720]	Specifies how long the switch waits between time polling intervals.	720 sec.	(page 29)	(page 36)
sntp server priority [1 - 3] *ip-address*	Specifies the order in which the configured servers are polled for getting the time.	-	(page 29)	-
sntp authentication key-id [*key-id*] authentication-mode md5 key-value *key-string* [trusted] no sntp authentication key-id [*key-id*]	Configures the key-id, authentication-mode, and key-value, which are required for authentication.	-	(page 31)	-
sntp authentication key-id *key-id* trusted	Configures a key-id as trusted	-	(page 32)	-
[no]sntp server priority [1-3] [*ip-address* | *ipv6-address*] *version-num* [key-id 1-4,294,967,295]	Configures a key-id to be associated with a specific server.	-	(page 32)	-
sntp authentication	Enables the SNTP client authentication	-	(page 33)	-

Table 1 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`show timep`	Lists both the time synchronization method (TimeP, SNTP, or None) and the TimeP configuration	-	(page 38)	-
`timesync timep`	Selects TimeP as the time protocol	-	(page 39)	-
`ip timep dhcp`	Configures DHCP as the TimeP mode	-	(page 39)	(page 44)
`ip timep manual` *`ip-addr`* `[ oobm ]`	Activates TimeP in manual mode with a specified TimeP server	-	(page 40)	(page 44)
`no ip timep`	Disables the TimeP mode	-	(page 40)	-
`ip timep[ dhcp | manual ]interval [1-9999]`	Specifies how long the switch waits between time polling intervals.	720 min.	(page 42)	(page 44)
`no sntp server` *`ip-addr`*	Deletes a server address.	-	(page 31)	-

General steps for running a time protocol on the switch

Using time synchronization ensures a uniform time among interoperating devices. This helps you to manage and troubleshoot switch operation by attaching meaningful time data to event and error messages.

The switch offers TimeP and SNTP (Simple Network Time Protocol) and a `timesync` command for changing the time protocol selection (or turning off time protocol operation).

NOTE: Although you can create and save configurations for both time protocols without conflicts, the switch allows only one active time protocol at any time.

In the factory-default configuration, the time synchronization option is set to TimeP, with the TimeP mode itself set to Disabled.

1. Select the time synchronization protocol: `SNTP` or `TimeP` (the default).
2. Enable the protocol; the choices are:
   - SNTP: `Broadcast` or `Unicast`
   - TimeP: `DHCP` or `Manual`
3. Configure the remaining parameters for the time protocol you selected.

   The switch retains the parameter settings for both time protocols even if you change from one protocol to the other. Thus, if you select a time protocol, the switch uses the parameters you last configured for the selected protocol.

Simply selecting a time synchronization protocol does not enable that protocol on the switch unless you also enable the protocol itself (step 2, above). For example, in the factory-default configuration, TimeP is the selected time synchronization method. However, because TimeP is disabled in the factory-default configuration, no time synchronization protocol is running.

Disabling time synchronization

You can use either of the following methods to disable time synchronization without changing the Timep or SNTP configuration:

- Global config level of the CLI
  - Execute `no timesync`.
- System Information screen of the Menu interface
  a. Set the `Time Synch Method` parameter to `None`.
  b. Press **[Enter]**, then **[S]** (for **Save**).

Viewing and configuring SNTP (CLI)

Syntax:

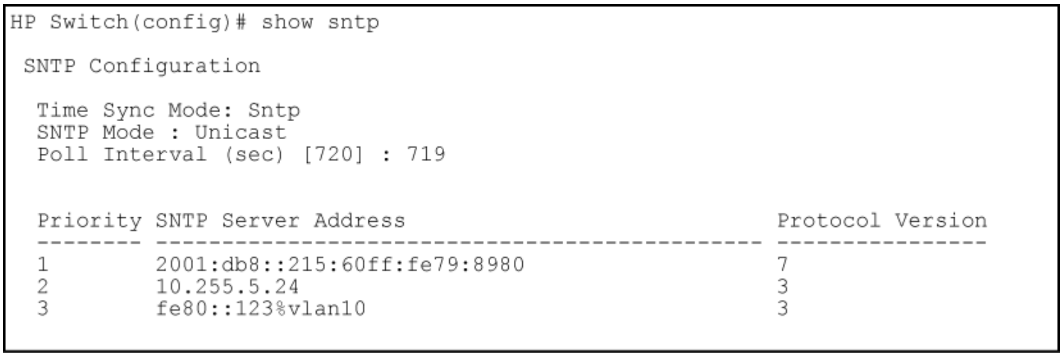
`show sntp`

Lists both the time synchronization method (`TimeP`, `SNTP`, or `None`) and the SNTP configuration, even if SNTP is not the selected time protocol.

Example

If you configure the switch with SNTP as the time synchronization method, then enable SNTP in broadcast mode with the default poll interval, `show sntp` lists the following:

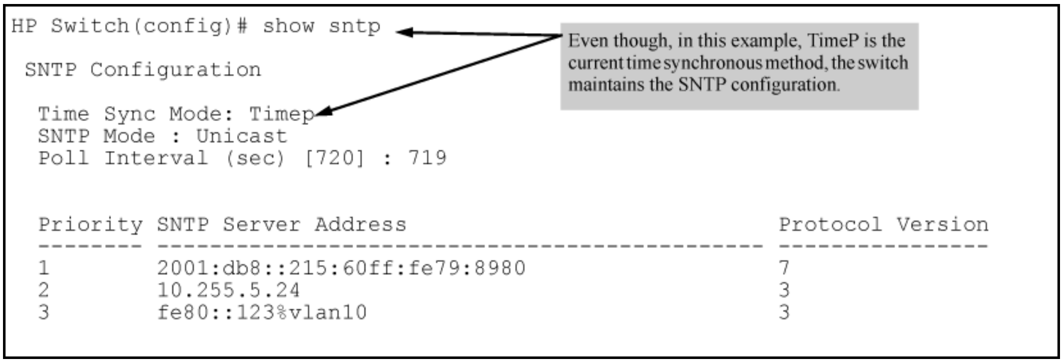
Figure 1 SNTP configuration when SNTP is the selected time synchronization method



```
HP Switch(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 719


  Priority SNTP Server Address                              Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                     7
  2        10.255.5.24                                      3
  3        fe80::123%vlan10                                 3
```

In the factory-default configuration (where TimeP is the selected time synchronization method), `show sntp` still lists the SNTP configuration, even though it is not currently in use.

Figure 2 SNTP configuration when SNTP is not the selected time synchronization method



```
HP Switch(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Timep
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 719


  Priority SNTP Server Address                              Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                     7
  2        10.255.5.24                                      3
  3        fe80::123%vlan10                                 3
```

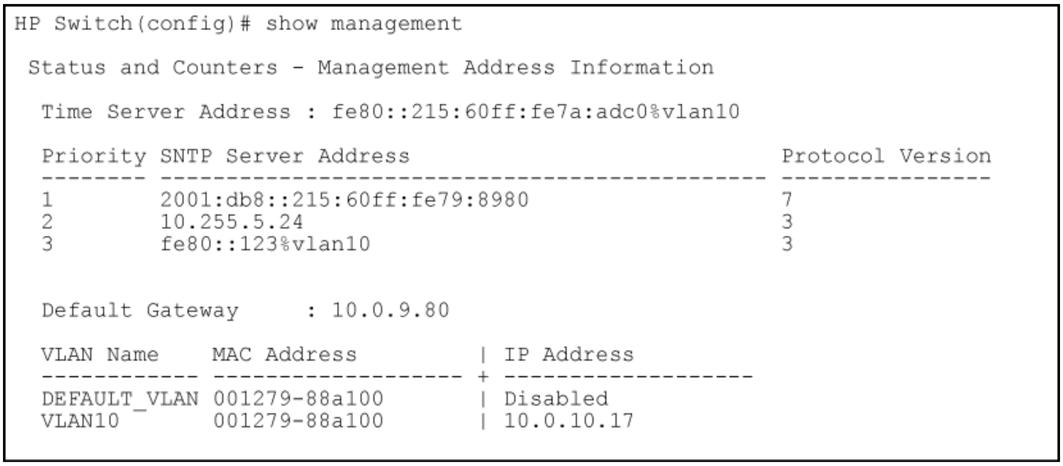
Even though, in this example, TimeP is the current time synchronous method, the switch maintains the SNTP configuration.

Syntax:

`show management`

This command can help you to easily examine and compare the IP addressing on the switch. It lists the IP addresses for all time servers configured on the switch, plus the IP addresses and default gateway for all VLANs configured on the switch.

Figure 3 Display showing IP addressing for all configured time servers and VLANs



```
HP Switch(config)# show management

 Status and Counters - Management Address Information

  Time Server Address : fe80::215:60ff:fe7a:adc0%vlan10

  Priority SNTP Server Address                              Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                     7
  2        10.255.5.24                                      3
  3        fe80::123%vlan10                                 3


  Default Gateway     : 10.0.9.80

  VLAN Name    MAC Address         | IP Address
  ------------ ------------------- + -------------------
  DEFAULT_VLAN 001279-88a100       | Disabled
  VLAN10       001279-88a100       | 10.0.10.17
```

Enabling or disabling the SNTP mode (CLI)

Disabling the SNTP Mode

If you want to prevent SNTP from being used even if it is selected by `timesync` (or the Menu interface's `Time Sync Method` parameter), configure the SNTP mode as disabled.

Syntax:

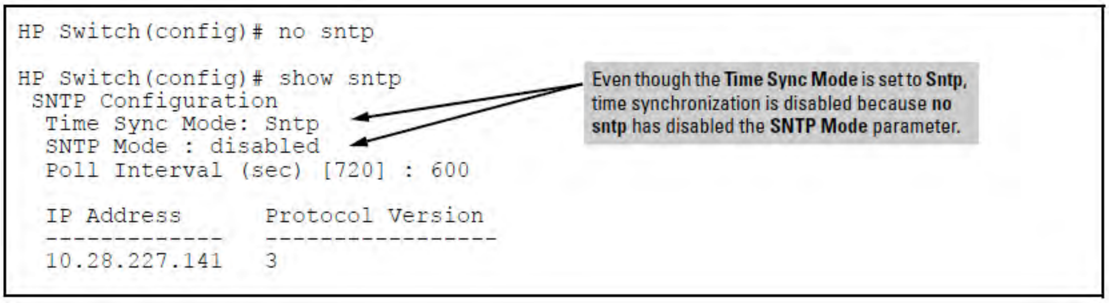
`no sntp`

Disables SNTP by changing the SNTP mode configuration to `Disabled`.

Example

If the switch is running SNTP in unicast mode with an SNTP server at 10.28.227.141 and a server version of 3 (the default), `no sntp` changes the SNTP configuration as shown below and disables time synchronization on the switch.

Figure 4 Disabling time synchronization by disabling the SNTP mode



```
HP Switch(config)# no sntp

HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Sntp
  SNTP Mode : disabled
  Poll Interval (sec) [720] : 600

  IP Address       Protocol Version
  -------------    -----------------
  10.28.227.141    3
```

Even though the **Time Sync Mode** is set to **Sntp**, time synchronization is disabled because **no sntp** has disabled the **SNTP Mode** parameter.

Configuring (enabling or disabling) the SNTP mode

Enabling the SNTP mode means to configure it for either broadcast or unicast mode. Remember that to run SNTP as the switch's time synchronization protocol, you must also select SNTP as the time synchronization method by using the CLI `timesync` command (or the menu interface **Time Sync Method** parameter.)

Syntax:

```
timesync sntp
```

Selects SNTP as the time protocol.

```
sntp <broadcast|unicast>
```

Enables the SNTP mode.

Syntax:

```
sntp server <ip-addr>
```

Required only for unicast mode.

Syntax

```
sntp server priority <1-3>
```

Specifies the order in which the configured servers are polled for getting the time. Value is between 1 and 3.

Syntax

```
sntp <30-720>
```

Configures the amount of time between updates of the system clock via SNTP.

Default: 720 seconds

Enabling SNTP in Broadcast Mode

Because the switch provides an SNTP polling interval (default:720 seconds), you need only these two commands for minimal SNTP broadcast configuration:

Syntax

```
timesync sntp
```

Selects SNTP as the time synchronization method.

Syntax

sntp broadcast

```
sntp broadcast
```

Configures broadcast as the SNTP mode.

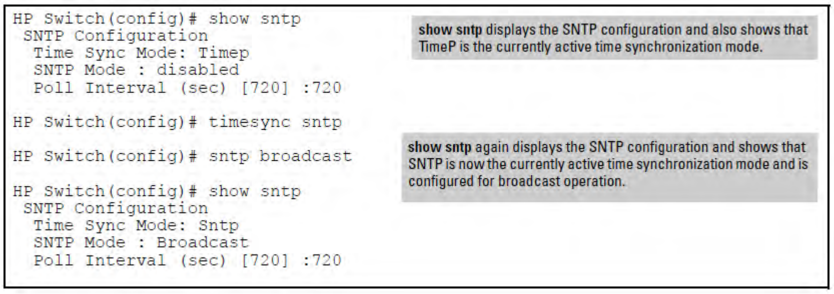
Example

Suppose that time synchronization is in the factory-default configuration (TimeP is the currently selected time synchronization method.) Complete the following:

1. View the current time synchronization.
2. Select **SNTP** as the time synchronization mode.
3. Enable **SNTP** for Broadcast mode.
4. View the SNTP confguration again to verify the configuration.

The commands and output would appear as follows:

Figure 5 Enabling SNTP operation in Broadcast Mode



```
HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Timep
  SNTP Mode : disabled
  Poll Interval (sec) [720] :720

HP Switch(config)# timesync sntp

HP Switch(config)# sntp broadcast

HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Sntp
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] :720
```

show sntp displays the SNTP configuration and also shows that TimeP is the currently active time synchronization mode.

show sntp again displays the SNTP configuration and shows that SNTP is now the currently active time synchronization mode and is configured for broadcast operation.

Configuring (enabling or disabling) in Broadcast mode

The switch provides an SNTP polling interval (default:720 seconds.) You need the two following commands for minimal SNTP broadcast configuration.

Syntax

```
timesync sntp
```

Selects SNTP as the time synchronization method.

Syntax

```
sntp broadcast
```

Configures broadcast as the SNTP mode.

Example

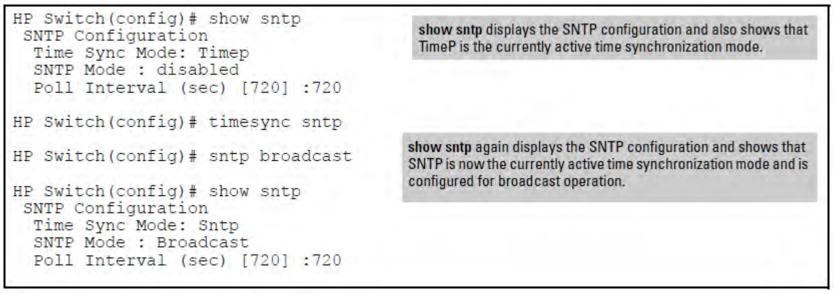
Suppose time synchronization is in the factory-default configuration (TimeP is the currently selected time synchronization method).

You want to:

1. View the current time synchronization: `show sntp` displays the SNTP configuration and also shows that TimeP is the currently active time synchronization mode.
2. Select SNTP as the time synchronization mode.
3. Enable SNTP for broadcast mode.
4. View the SNTP configuration again to verify the configuration.

The commands and output appear as follows:

Figure 6 `show sntp` configuration output



```
HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Timep
  SNTP Mode : disabled
  Poll Interval (sec) [720] :720

HP Switch(config)# timesync sntp

HP Switch(config)# sntp broadcast

HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Sntp
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] :720
```

show sntp displays the SNTP configuration and also shows that TimeP is the currently active time synchronization mode.

show sntp again displays the SNTP configuration and shows that SNTP is now the currently active time synchronization mode and is configured for broadcast operation.

Enabling SNTP in unicast mode (CLI)

Like broadcast mode, configuring SNTP for unicast mode enables SNTP. However, for unicast operation, you must also specify the IP address of at least one SNTP server. The switch allows up to three unicast servers. You can use the Menu interface or the CLI to configure one server or to replace an existing unicast server with another. To add a second or third server, you must use the

CLI. For more on SNTP operation with multiple servers, see "About SNTP unicast time polling with multiple SNTP servers" (page 46)

Syntax:

`timesync sntp`

Selects SNTP as the time synchronization method.

`sntp unicast`

Configures the SNTP mode for unicast operation.

Syntax:

`[no] sntp server priority [ 1-3 ]` *`ip-address`* `[ oobm ][ version ]`

Use the no version of the command to disable SNTP.

`priority` Specifies the order in which the configured SNTP servers are polled for the time.

`ip-address` An IPv4 or IPv6 address of an SNTP server.

`oobm` For switches that have a separate out-of-band management port, specifies that SNTP traffic goes through that port. (By default, SNTP traffic goes through the data ports.)

`version` The protocol version of the SNTP server. Allowable values are 1 through 7; default is 3.

Syntax:

`no sntp server <`*`ip-addr`*`>`

Deletes the specified SNTP server.

NOTE: Deleting an SNTP server when only one is configured disables SNTP unicast operation.

Example

To select SNTP and configure it with unicast mode and an SNTP server at 10.28.227.141 with the default server version (3) and default poll interval (720 seconds):

```
HP Switch(config)# timesync sntp
```

Selects SNTP.

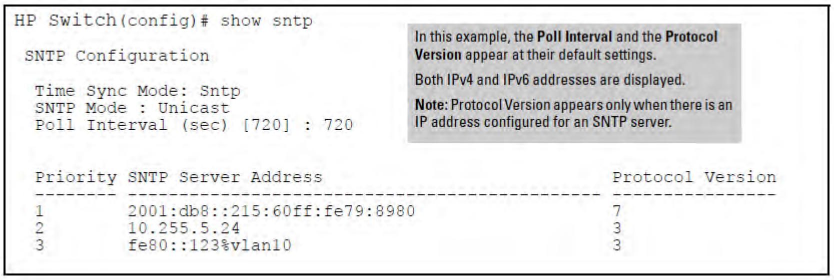
```
HP Switch(config)# sntp unicast
```

Activates SNTP in unicast mode.

```
HP Switch(config)# sntp server priority 1
10.28.227.141
```

Specifies the SNTP server and accepts the current SNTP server version (default: 3).

Figure 7 Configuring SNTP for unicast operation



```
HP Switch(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 720


  Priority SNTP Server Address                              Protocol Version
  -------- ---------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                     7
  2        10.255.5.24                                      3
  3        fe80::123%vlan10                                 3
```

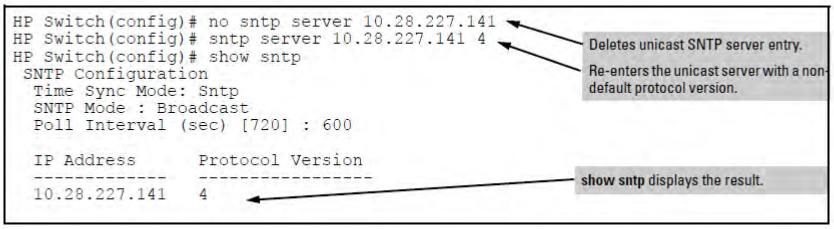
In this example, the **Poll Interval** and the **Protocol Version** appear at their default settings.

Both IPv4 and IPv6 addresses are displayed.

Note: Protocol Version appears only when there is an IP address configured for an SNTP server.

If the SNTP server you specify uses SNTP v4 or later, use the `sntp server` command to specify the correct version number. For example, suppose you learned that SNTP v4 was in use on the server you specified above (IP address 10.28.227.141). You would use the following commands to delete the server IP address , re-enter it with the correct version number for that server

Figure 8 Specifying the SNTP protocol version number



```
HP Switch(config)# no sntp server 10.28.227.141
HP Switch(config)# sntp server 10.28.227.141 4
HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Sntp
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] : 600

  IP Address      Protocol Version
  -------------   -----------------
  10.28.227.141   4
```

Deletes unicast SNTP server entry.

Re-enters the unicast server with a non-default protocol version.

show sntp displays the result.

SNTP unitcast time polling with multiple SNTP servers

When running SNTP unicast time polling as the time synchronization method, the switch requests a time update from the server you configured with either the server address parameter in the menu interface, or the primary server in a list of up to three SNTP servers configured using the CLI. If the switch does not receive a response from the primary server after three consecutive polling intervals, the switch tries the next server (if any) in the list. If the switch tries all servers in the list without success, it sends an error message to the Event Log and reschedules to try the address list again after the configured `Poll Interval` time has expired.

Changing the SNTP poll interval (CLI)

Syntax:

`sntp <30..720>`

Specifies the amount of time between updates of the system clock via SNTP. The default is 720 seconds and the range is 30 to 720 seconds. (This parameter is separate from the poll interval parameter used for Timep operation.)

Example

To change the poll interval to 300 seconds:

```
HP Switch(config)# sntp 300
```

Changing the SNTP server priority (CLI)

You can choose the order in which configured servers are polled for getting the time by setting the server priority.

Syntax:

`sntp server priority <1 - 3>` *`<ip-address>`*

Specifies the order in which the configured servers are polled for getting the time Value is between 1 and 3.

NOTE: You can enter both IPv4 and IPv6 addresses. For more information about IPv6 addresses, see the *IPv6 Configuration Guide* for your switch.

Example

To set one server to priority 1 and another to priority 2:

```
HP Switch(config)# sntp server priority 1 10.28.22.141
HP Switch(config)# sntp server priority 2
                2001:db8::215:60ff:fe79:8980
```

Disabling time synchronization without changing the SNTP configuration (CLI)

The recommended method for disabling time synchronization is to use the `timesync` command.

Syntax:

`no timesync`
Halts time synchronization without changing your SNTP configuration.

Example

Suppose SNTP is running as the switch's time synchronization protocol, with `broadcast` as the SNTP mode and the factory-default polling interval. You would halt time synchronization with this command:

```
HP Switch(config)# no timesync
```

If you then viewed the SNTP configuration, you would see the following:

Example 1 SNTP with time synchronization disabled

```
HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Disabled
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] : 720
```

Displaying all SNTP server addresses configured on the switch (CLI)

The System Information screen in the menu interface displays only one SNTP server address, even if the switch is configured for two or three servers. The CLI `show management` command displays all configured SNTP servers on the switch.

Example 2 Example of how to list all SNTP servers configured on the switch

```
HP Switch(config)# show management

 Status and Counters - Management Address Information

  Time Server Address : fe80::215:60ff:fe7a:adc0%vlan10

  Priority SNTP Server Address Protocol Version
  -------- ---------------------------------------------- ----------------
  1 2001:db8::215:60ff:fe79:8980 7
  2 10.255.5.24 3
  3 fe80::123%vlan10 3


  Default Gateway : 10.0.9.80

  VLAN Name    MAC Address         | IP Address
  ------------ ------------------- + -------------------
  DEFAULT_VLAN 001279-88a100       | Disabled
  VLAN10       001279-88a100       | 10.0.10.17
```

Adding and deleting SNTP server addresses

Adding addresses

As mentioned earlier, you can configure one SNTP server address using either the Menu interface or the CLI. To configure a second and third address, you must use the CLI. To configure the remaining two addresses, you would do the following:

Example 3 Example of creating additional SNTP server addresses with the CLI

```
HP Switch(config)# sntp server 2001:db8::215:60ff:fe79:8980
HP Switch(config)# sntp server 10.255.5.24
```

NOTE: If there are already three SNTP server addresses configured on the switch, and you want to use the CLI to replace one of the existing addresses with a new one, you must delete the unwanted address before you configure the new one.

Deleting addresses

Syntax:

`no sntp server priority 1-3` *`ip-addr`*

Deletes a server address. If there are multiple addresses and you delete one of them, the switch re-orders the address priority.

Example

To delete the primary address in the above example and automatically convert the secondary address to primary:

```
HP Switch(config)# no sntp server 10.28.227.141
```

Configuring the key-identifier, authentication mode, and key-value (CLI)

This command configures the `key-id`, `authentication-mode`, and `key-value`, which are required for authentication. It is executed in the global configuration context.

For detailed information on client authentication, see “About SNTP: Selecting and configuring” (page 45).

Syntax:

```
sntp authentication key-id key-id authentication-mode md5 key-value
key-string trusted [encrypted-key key-string]
no sntp authentication key-id key-id
```

Configures a key-id, authentication-mode (MD5 only), and key-value, which are required for authentication.

The `no` version of the command deletes the authentication key.

Default: No default keys are configured on the switch.

`key-id` A numeric key identifier in the range of 1-4,294,967,295 (2^{32}) that identifies the unique key value. It is sent in the SNTP packet.

`key-value` *`key-string`* The secret key that is used to generate the message digest. Up to 32 characters are allowed for *`key-string`*.

NOTE: For the 5400zl, 3800, and 8200zl switches, when the switch is in enhanced secure mode, commands that take a secret key as a parameter have the echo of the secret typing replaced with asterisks. The input for <key-string> is prompted for interactively. For more information, see the chapter “Secure Mode (5400zl and 8200zl Switches)” in the *Access Security Guide* for your switch.

`encrypted-key` *`key-string`* Set the SNTP authentication key value using a base64–encoded aes-256 encrypted string.

Example 4 Example of setting parameters for SNTP authentication

```
HP Switch(config)# sntp authentication key-id 55 authentication-mode md5 key-value secretkey1
```

Configuring a `key-id` as `trusted` (CLI)

Enter the following command to configure a key-id as trusted.

Syntax:

```
sntp authentication key-id key-id trusted
no sntp authentication key-id key-id trusted
```

Trusted keys are used during the authentication process. You can configure the switch with up to eight sets of key-id/key-value pairs. One specific set must selected for authentication; this is done by configuring the set as `trusted`.

The `key-id` itself must already be configured on the switch. To enable authentication, at least one `key-id` must be configured as `trusted`.

The `no` version of the command indicates the key is unreliable (not trusted).

Default: No key is trusted by default.

For detailed information about trusted keys, see “About configuring a trusted key” (page 48)

Associating a key with an SNTP server (CLI)

Syntax:

```
[no] sntp server priority 1-3 ip-address | ipv6-address
version-num [ key-id 1-4,294,967,295 ]
```

Configures a `key-id` to be associated with a specific server. The key itself must already be configured on the switch.

The `no` version of the command disassociates the key from the server. This does not remove the authentication key.

Default: No key is associated with any server by default.

`priority` Specifies the order in which the configured servers are polled for getting the time.

`version-num` Specifies the SNTP software version to use and is assigned on a per-server basis. The version setting is backwards-compatible. For example, using version 3 means that the switch accepts versions 1 through 3. Default: 3; range: 1 - 7.

`key-id` Optional command. The key identifier sent in the SNTP packet. This `key-id` is associated with the SNTP server specified in the command.

Example 5 Example of associating a `key-id` with a specific server

```
HP Switch(config)# sntp server priority 1 10.10.19.5 2 key-id 55
```

Enabling SNTP client authentication (CLI)

Enabling SNTP authentication allows network devices such as HP switches to validate the SNTP messages received from an NTP or SNTP server before updating the network time. NTP or SNTP servers and clients must be configured with the same set of authentication keys so that the servers can aithenticate the messages they send and clients (HP switches) can validate the received messages before updating the time.

This feature provides support for SNTP client authentication on HP switches, which addresses security considerations when deploying SNTP in a network.

Requirements to enable SNTP client authentication

The following must be configured to enable SNTP client authentication on the switch.

SNTP client Authentication Support

- Timesync mode must be SNTP. Use the timesync sntp command. (SNTP is disabled by default.)
- SNTP must be in unicast or broadcast mode. See “Configuring Unicast and Broadcast Mode” on page 1-19.
- The MD5 authentication mode must be selected.
- An SNTP authentication key-identifier (`key-id`) must be configured on the switch and a value (`key-value`) must be provided for the authentication key. A maximum of 8 sets of `key-id` and `key-value` can be configured on the switch.
- Among the keys that have been configured, one key or a set of keys must be configured as trusted. Only trusted keys will be used for SNTP authentication.
- If the SNTP server requires authentication, one of the trusted keys has to be associated with the SNTP server.
- SNTP client authentication must be enabled on the HP switch. If client authentication is disabled, packets are processed without authentication. All of the above steps are necessary to enable authentication on the client.

SNTP server authentication support

The following must be performed on the SNTP server:

- The same authentication key-identifier, trusted key, authentication mode and key-value that were configured on the SNTP client must also be configured on the SNTP server.
- SNTP server authentication must be enabled on the server.If any of the parameters on the server are changed, the parameters have to be changed on all the SNTP clients in the network as well. The authentication check will fail on the clients otherwise, and the SNTP packets will be dropped.

NOTE: SNTP server is not supported on HP products.

Enabling SNTP Client Authentication

The `sntp authentication` command enables SNTP client authentication on the switch. If SNTP authentication is not enabled, SNTP packets are not authenticated.

Syntax:

```
[no] sntp authentication
```

Enables the SNTP client authentication.

The `no` version of the command disables authentication.

Default: SNTP client authentication is disabled.

Configuring unicast and broadcast mode for authentication

To enable authentication, you must configure either unicast or broadcast mode. When authentication is enabled, changing the mode from unicast to broadcast or vice versa is not allowed; you must disable authentication and then change the mode.

To set the SNTP mode or change from one mode to the other, enter the appropriate command.

Syntax:

```
sntp unicast
sntp broadcast
```

Enables SNTP for either broadcast or unicast mode.

Default: SNTP mode is disabled by default. SNTP does not operate even if specified by the CLI `timesync` command or by the menu interface `Time Sync Method` parameter.

`Unicast` Directs the switch to poll a specific server periodically for SNTP time synchronization.

The default value between each polling request is 720 seconds, but can be configured.

At least one manually configured server IP address is required.

NOTE: At least one `key-id` must be configured as `trusted`, and it must be associated with one of the SNTP servers. To edit or remove the associated `key-id` information or SNTP server information, SNTP authentication must be disabled.

`Broadcast` Directs the switch to acquire its time synchronization from data broadcast by any SNTP server to the network broadcast address. The switch uses the first server detected and ignores any others. However, if the Poll Interval (configurable up to 720 seconds) expires three times without the switch detecting a time update from the original server, the switch accepts a broadcast time update from the next server it detects.

Viewing SNTP authentication configuration information (CLI)

The `show sntp` command displays SNTP configuration information, including any SNTP authentication keys that have been configured on the switch.

Example 6 Example of SNTP configuration information

```
HP Switch(config)# show sntp

 SNTP Configuration

  SNTP Authentication : Enabled
  Time Sync Mode: Sntp
  SNTP Mode : Unicast
  Poll Interval (sec) [720] : 720

  Priority SNTP Server Address                       Protocol Version KeyId
  -------- --------------------------------------- ---------------- -----
  1        10.10.10.2                                3                55
  2        fe80::200:24ff:fec8:4ca8                  3                55
```

Example 7 `show sntp authentication` command output

To display all the SNTP authentication keys that have been configured on the switch, enter the `show sntp authentication` command.

```
HP Switch (config) # show sntp authentication
SNTP Authentication Information
SNTP Authentication: Enabled
Key-ID                Auth Mode              Trusted
-------              -----------             -------
55                       MD5                  YES
10                       MD5                   NO
```

To display the statistical information for each SNTP server, enter the `sntp statistics` command. The number of SNTP packets that have failed authertication is displayed for each SNTP server address.

```
HP Switch (config) # show sntp statistics
SNTP statistics
Received Packets:   0
Sent Packets:       3
Dropped Packets:    0

SNTP Server Address                   Auth Failed Pkts
-------------------                   ----------------
10.10.10.1                                0
fe80::200:24ff:fec8:4ca8                  0
```

Viewing all SNTP authentication keys that have been configured on the switch (CLI)

Enter the `show sntp authentication` command, as shown in Example 8.

Example 8 Example of show sntp authentication command output

```
HP Switch(config)# show sntp authentication

  SNTP Authentication Information

  SNTP Authentication : Enabled

  Key-ID  Auth Mode  Trusted
  ------- ---------- --------
  55      MD5        Yes
  10      MD5        No
```

Viewing statistical information for each SNTP server (CLI)

To display the statistical information for each SNTP server, enter the `show sntp statistics` command.

The number of SNTP packets that have failed authentication is displayed for each SNTP server address, as shown in Example 9.

Example 9 Example of SNTP authentication statistical information

```
HP Switch(config)# show sntp statistics
SNTP Statistics

  Received Packets : 0
  Sent Packets : 3
  Dropped Packets : 0

  SNTP Server Address                     Auth Failed Pkts
  --------------------------------------- ----------------
  10.10.10.1                                  0
  fe80::200:24ff:fec8:4ca8                    0
```

Storing security information in the running-config file (CLI)

Enter the `include-credentials` command.

For more information and examples, see "About saving configuration files and the `include-credentials` command" (page 48).

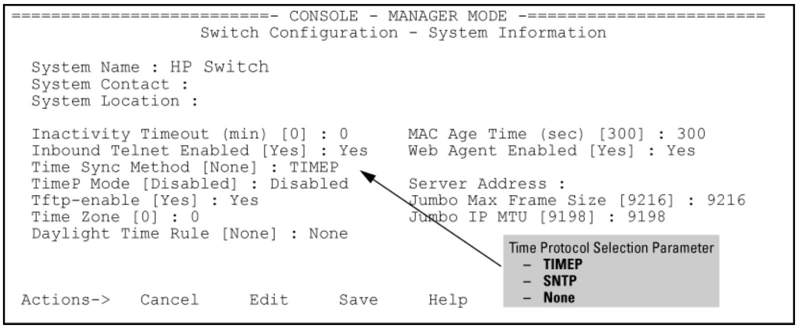
Viewing and configuring SNTP (Menu)

1. From the Main Menu, select:

   2. Switch Configuration…

   1. System Information

   ### Figure 9 System Information screen (default values)



```
=========================- CONSOLE - MANAGER MODE -=======================
                  Switch Configuration - System Information

  System Name : HP Switch
  System Contact :
  System Location :

  Inactivity Timeout (min) [0] : 0      MAC Age Time (sec) [300] : 300
  Inbound Telnet Enabled [Yes] : Yes    Web Agent Enabled [Yes] : Yes
  Time Sync Method [None] : TIMEP
  TimeP Mode [Disabled] : Disabled      Server Address :
  Tftp-enable [Yes] : Yes               Jumbo Max Frame Size [9216] : 9216
  Time Zone [0] : 0                     Jumbo IP MTU [9198] : 9198
  Daylight Time Rule [None] : None


 Actions->   Cancel     Edit     Save     Help
```

Time Protocol Selection Parameter
- **TIMEP**
- **SNTP**
- **None**

2. Press **[E]** (for **Edit**).

   The cursor moves to the **System Name** field.

3. Use â to move the cursor to the **Time Sync Method** field.
4. Use the **Space** bar to select **SNTP**, then press â once to display and move to the **SNTP Mode** field.
5. Complete one of the following options.

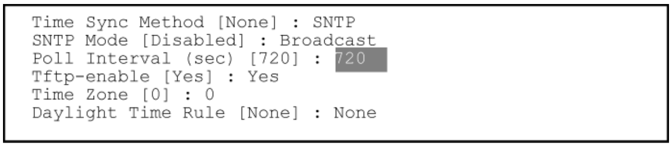
Option 1

a. Use the **Space** bar to select the **Broadcast** mode.

b. Press â to move the cursor to the **Poll Interval** field.

c. Go to step 6 (page 37). (For Broadcast mode details, see“About SNTP time synchronization” (page 45))

Figure 10 Time configuration fields for SNTP with broadcast mode



```
Time Sync Method [None] : SNTP
SNTP Mode [Disabled] : Broadcast
Poll Interval (sec) [720] : 720
Tftp-enable [Yes] : Yes
Time Zone [0] : 0
Daylight Time Rule [None] : None
```

Option 2

d. Use the Space bar to select the **Unicast** mode.

e. Press **à** to move the cursor to the **Server Address** field.

f. Enter the IP address of the SNTP server you want the switch to use for time synchronization.

NOTE: This step replaces any previously configured server IP address. If you will be using backup SNTP servers (requires use of the CLI), see“About SNTP unicast time polling with multiple SNTP servers” (page 46).

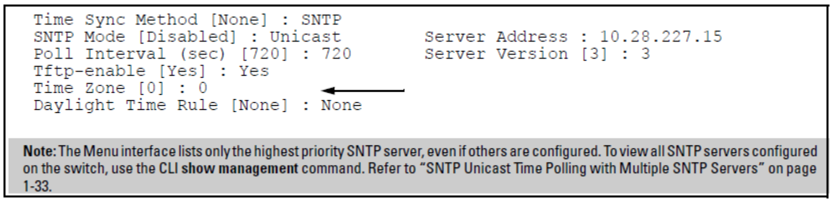
g. Press â to move the cursor to the **Server Version** field. Enter the value that matches the SNTP server version running on the device you specified in the preceding step .

If you are unsure which version to use, HP recommends leaving this value at the default setting of 3 and testing SNTP operation to determine whether any change is necessary.

NOTE: Using the menu to enter the IP address for an SNTP server when the switch already has one or more SNTP servers configured, the switch deletes the primary SNTP server from the server list. The switch then selects a new primary SNTP server from the IP addresses in the updated list. For more on this topic, see“About SNTP unicast time polling with multiple SNTP servers” (page 46).

h. Press à to move the cursor to the **Poll Interval** field, then go to step 6.

Figure 11 SNTP configuration fields for SNTP configured with unicast mode



```
Time Sync Method [None] : SNTP
SNTP Mode [Disabled] : Unicast           Server Address : 10.28.227.15
Poll Interval (sec) [720] : 720          Server Version [3] : 3
Tftp-enable [Yes] : Yes
Time Zone [0] : 0
Daylight Time Rule [None] : None
```

Note: The Menu interface lists only the highest priority SNTP server, even if others are configured. To view all SNTP servers configured on the switch, use the CLI **show management** command. Refer to “SNTP Unicast Time Polling with Multiple SNTP Servers” on page 1-33.

6. In the **Poll Interval** field, enter the time in seconds that you want for a Poll Interval.

   (For Poll Interval operation, see Table 2 (page 45), on “SNTP parameters” (page 45).)

7. Press **Enter** to return to the Actions line, then **S** (for **Save**) to enter the new time protocol configuration in both the startup-config and running-config files.

Viewing the current TimeP configuration (CLI)

Using different `show` commands, you can display either the full TimeP configuration or a combined listing of all TimeP, SNTP, and VLAN IP addresses configured on the switch.

Syntax:

```
show timep
```

Lists both the time synchronization method (TimeP, SNTP, or None) and the TimeP configuration, even if SNTP is not the selected time protocol. (If the TimeP Mode is set to `Disabled` or `DHCP`, the Server field does not appear.)

Example

Example 10 TimeP configuration when TimeP is the selected Time synchronization method

If you configure the switch with TimeP as the time synchronization method, then enable TimeP in DHCP mode with the default poll interval, `show timep` lists the following:

```
HP Switch(config)# show timep

 Timep Configuration

  Time Sync Mode: Timep
  TimeP Mode [Disabled] : DHCP    Server Address : 10.10.28.103
  Poll Interval (min) [720] : 720
```

Example 11 TimeP configuration when TimeP is not the selected time synchronization method

If SNTP is the selected time synchronization method, `show timep` still lists the TimeP configuration even though it is not currently in use. Even though, in this example, SNTP is the current time synchronization method, the switch maintains the TimeP configuration (see data in bold below):

```
HP Switch(config)# show timep

 Timep Configuration

  Time Sync Mode: Sntp
  TimeP Mode [Disabled] : Manual   Server Address : 10.10.28.100
  Poll Interval (min) [720] : 720
```

Syntax:

```
show management
```

Helps you to easily examine and compare the IP addressing on the switch. It lists the IP addresses for all time servers configured on the switch plus the IP addresses and default gateway for all VLANs configured on the switch.

Example 12 Example of display showing IP addressing for all configured time servers and VLANs

```
HP Switch(config)# show management

 Status and Counters - Management Address Information

  Time Server Address : 10.10.28.100

  Priority SNTP Server Address                            Protocol Version
  -------- ---------------------------------------------- ----------------
  1        10.10..28.101                                  3
  2        10.255.5.24                                    3
  3        fe80::123%vlan10                               3


  Default Gateway : 10.0.9.80

  VLAN Name    MAC Address         | IP Address
  ------------ ------------------- + -------------------
  DEFAULT_VLAN 001279-88a100       | 10.30.248.184
  VLAN10 001279-88a100             | 10.0.10.17
```

Configuring (Enabling or Disabling) the TimeP mode

Enabling the TimeP mode means to configure it for either broadcast or unicast mode. Remember to run TimeP as the switch's time synchronization protocol, you must also select TimeP as the time synchronization method by using the CLI `timesync` command (or the menu interface **Time Sync Method** parameter.

Syntax:

`timesync timep`

Selects TimeP as the time synchronization method.

Syntax:

`ip timep <dhcp|manual>`

Enables the selected TimeP mode.

Syntax

`[no]ip timep`

Disables the TimeP mode.

Syntax

`[no]timesync`

Disables the time protocol.

Example

Suppose time synchronization is configured for SNTP. You want to:

1. View the current time synchronization.

   `show timep` displays the TimeP configuration and also shows that SNTP is the currently active time synchronization mode.

2. Select TimeP as the time synchronization mode.
3. Enable TimeP for DHCP mode.

4. View the TimeP configuration.

   `show timep` again displays the TimeP configuration and shows that TimeP is now the currently active time synchronization mode.

The commands and output appear as follows:

Enabling TimeP operation in DHCP mode

```
HP Switch(config)# show timep

 Timep Configuration

  Time Sync Mode: Sntp
  TimeP Mode : Disabled
  Poll Interval (min) [720] : 720

HP Switch(config)# timesync timep

HP Switch(config)# ip timep dhcp

HP Switch(config)# show timep

 Timep Configuration
  Time Sync Mode: Timep
  TimeP Mode : DHCP Poll Interval (min): 720
```

Enabling TimeP in manual mode (CLI)

Like DHCP mode, configuring TimeP for `manual` mode enables TimeP. However, for manual operation, you must also specify the IP address of the TimeP server. (The switch allows only one TimeP server.)

Syntax:

`timesync timep`

Selects TimeP.

Syntax:

`ip timep manual` *`ip-addr`* `[ oobm ]`

Activates TimeP in manual mode with a specified TimeP server.

For switches that have a separate out-of-band management port, `oobm` specifies that SNTP traffic goes through that port. (By default, SNTP traffic goes through the data ports.)

Syntax:

`no ip timep`

Disables TimeP.

Enabling TimeP in DHCP Mode

Because the switch provides a TimeP polling interval (default:720 minutes), you need only these two commands for a minimal TimeP DHCP configuration:

Syntax

`timesync timep`

Selects TimeP as the time synchronization method.

Syntax

`ip timep dhcp`

Configures DHCP as the TimeP mode.

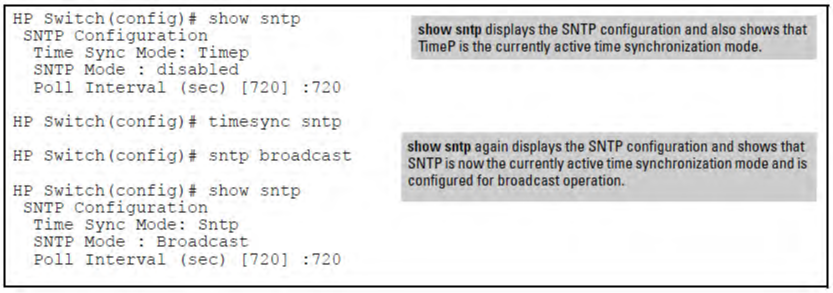
Example 13 TimeP synchronization method

Suppose:

- Time Synchronization is configured for SNTP.
- You want to:
  - View the current time synchronization.
  - Select TimeP as the synchronization mode.
  - Enable TimeP for DHCP mode.
  - View the TimeP configuration.

The commands and output would appears as follows:

Figure 12 Enabling TimeP operation in DHCP mode



```
HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Timep
  SNTP Mode : disabled
  Poll Interval (sec) [720] :720

HP Switch(config)# timesync sntp

HP Switch(config)# sntp broadcast

HP Switch(config)# show sntp
 SNTP Configuration
  Time Sync Mode: Sntp
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] :720
```

show sntp displays the SNTP configuration and also shows that TimeP is the currently active time synchronization mode.

show sntp again displays the SNTP configuration and shows that SNTP is now the currently active time synchronization mode and is configured for broadcast operation.

Enabling TimeP in Manual Mode

Like DHCP mode, configuring TimeP for Manual Mode enables TimeP. However, for manual operation, you must also specify the IP address of the TimeP server. (The switch allows only one TimeP server.) To enable the TimeP protocol:

Syntax

`timesync timep`

Selects TimeP.

Syntax

`ip timep manual <ip-addr> [oobm]`

Activates TimeP in manual mode with a specified TimeP server.

For switches that have a separate out-of-band management port, oobm specifies that SNTP traffic goes through that port. (By default, SNTP traffic goes through the data ports.)

Syntax

`[no]ip timep`

Disables TimeP.

NOTE: To change from one TimeP server to another, you must use the `no ip timep` command to disable TimeP mode, the reconfigure TimeP in manual mode with the new server IP address.

Example

To select TimeP and configure it for manual operation using a TimeP server address of 10.28.227.141 and the default poll interval (720 minutes, assuming the TimeP poll interval is already set to the default):

```
HP Switch(config)# timesync time
```

Selects TimeP.

```
HP Switch(config)# ip timep manual 10.28.227.141
```

Activates TimeP in Manual mode.

Example 14 Configuring TimeP for manual operation

```
HP Switch(config)# timesync timep
HP Switch(config)# ip timep manual 10.28.227.141

HP Switch(config)# show timep
 Timep Configuration

  Time Sync Mode: Timep
  TimeP Mode :  Manual              Server Address : 10.28.227.141
  Poll Interval (min) : 720
```

Changing from one TimeP server to another (CLI)

1. Use the `no ip timep` command to disable TimeP mode.
2. Reconfigure TimeP in Manual mode with the new server IP address.

Changing the TimeP poll interval (CLI)

Syntax:

```
ip timep   dhcp | manual   interval  [ 1-9999 ]
```

Specifies how long the switch waits between time polling intervals. The default is 720 minutes and the range is 1 to 9999 minutes. (This parameter is separate from the `poll interval` parameter used for SNTP operation.)

Example

To change the poll interval to 60 minutes:

```
HP Switch(config)# ip timep interval 60
```

Disabling time synchronization without changing the TimeP configuration (CLI)

Syntax:

```
no timesync
```

Disables time synchronization by changing the `Time Sync Mode` configuration to `Disabled`. This halts time synchronization without changing your TimeP configuration.The recommended method for disabling time synchronization is to use the `timesync` command.

Example

Suppose TimeP is running as the switch's time synchronization protocol, with `DHCP` as the TimeP mode, and the factory-default polling interval. You would halt time synchronization with this command:

```
HP Switch (config)# no timesync
```

If you then viewed the TimeP configuration, you would see the following:

Example 15 TimeP with time synchronization disabled

```
HP Switch(config)# show timep

 Timep Configuration
  Time Sync Mode: Disabled
  TimeP Mode : DHCP Poll Interval (min): 720
```

Disabling the TimeP mode

Syntax:

```
no ip timep
```

Disables TimeP by changing the TimeP mode configuration to `Disabled` and prevents the switch from using it as the time synchronization protocol, even if it is the selected `Time Sync Method` option.

Example

If the switch is running TimeP in DHCP mode, `no ip timep` changes the TimeP configuration as shown below and disables time synchronization. Even though the TimeSync mode is set to TimeP, time synchronization is disabled because `no ip timep` has disabled the TimeP mode parameter.

Example 16 Disabling time synchronization by disabling the TimeP mode parameter

```
HP Switch(config)# no ip timep

HP Switch(config)# show timep

 Timep Configuration
  Time Sync Mode: Timep
  TimeP Mode : Disabled
```

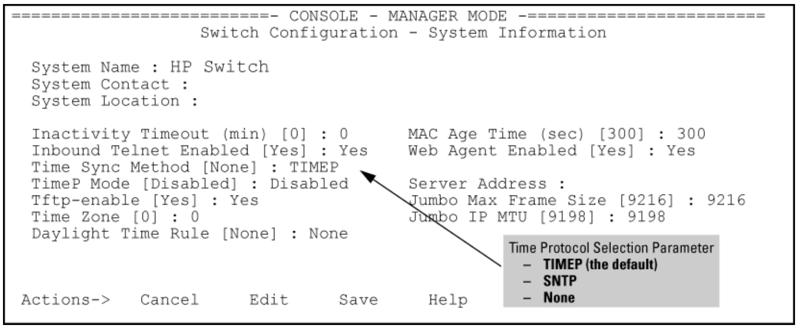
Viewing, enabling, and modifying the TimeP protocol (Menu)

1. From the Main Menu, select:

   2. Switch Configuration

   1. System Information

   ### Figure 13 System Information screen (default values)

   ```
   =========================- CONSOLE - MANAGER MODE -========================
                        Switch Configuration - System Information

     System Name : HP Switch
     System Contact :
     System Location :

     Inactivity Timeout (min) [0] : 0      MAC Age Time (sec) [300] : 300
     Inbound Telnet Enabled [Yes] : Yes    Web Agent Enabled [Yes] : Yes
     Time Sync Method [None] : TIMEP
     TimeP Mode [Disabled] : Disabled      Server Address :
     Tftp-enable [Yes] : Yes               Jumbo Max Frame Size [9216] : 9216
     Time Zone [0] : 0                     Jumbo IP MTU [9198] : 9198
     Daylight Time Rule [None] : None


    Actions->   Cancel     Edit     Save     Help
   ```

   Time Protocol Selection Parameter
   - **TIMEP (the default)**
   - **SNTP**
   - **None**

2. Press **[E]** (for **Edit**).

   The cursor moves to the **System Name** field.
3. Use **â** to move the cursor to the **Time Sync Method** field.
4. If **TIMEP** is not already selected, use the **Space** bar to select **TIMEP**, then press **â** once to display and move to the **TIMEP Mode** field.
5. Do one of the following:
   - Use the **Space** bar to select the **DHCP** mode.
     - Press **â** to move the cursor to the **Poll Interval** field.
     - Go to step 6.

Enabling TIMEP or DHCP

```
Time Sync Method [None] :   TIMEP
TimeP Mode [Disabled] :     DHCP
Poll Interval (min) [720] : 720
```

```
Time Zone [0] :            0
Daylight Time Rule [None] : None
```

- Use the **Space**bar to select the **Manual** mode.
  - Press **à** to move the cursor to the **Server Address** field.
  - Enter the IP address of the TimeP server you want the switch to use for time synchronization.

    NOTE: This step replaces any previously configured TimeP server IP address.

  - Press **à** to move the cursor to the **Poll Interval** field, then go to step 6.

6. In the **Poll Interval** field, enter the time in minutes that you want for a TimeP Poll Interval.
7. Select **[Enter]** to return to the **Actions** line, then select **[S]** (for **Save**) to enter the new time protocol configuration in both the startup-config and running-config files.

About SNTP time synchronization

SNTP provides two operating modes:

- **Broadcast mode**

  The switch acquires time updates by accepting the time value from the first SNTP time broadcast detected. (In this case, the SNTP server must be configured to broadcast time updates to the network broadcast address; see the documentation provided with your SNTP server application.) Once the switch detects a particular server, it ignores time broadcasts from other SNTP servers unless the configurable Poll Interval expires three consecutive times without an update received from the first-detected server.

  NOTE: To use Broadcast mode, the switch and the SNTP server must be in the same subnet.

- **Unicast mode**

  The switch requests a time update from the configured SNTP server. (You can configure one server using the menu interface, or up to three servers using the CLI sntp server command.) This option provides increased security over the Broadcast mode by specifying which time server to use instead of using the first one detected through a broadcast.

About SNTP: Selecting and configuring

Table 2 (page 45) shows the SNTP parameters and their operations.

Table 2 SNTP parameters

SNTP parameter	Operation
Time Sync Method	Used to select either SNTP, TIMEP, or None as the time synchronization method.
SNTP Mode	
`Disabled`	The Default. SNTP does not operate, even if specified by the Menu interface **Time Sync Method** parameter or the CLI `timesync` command.
`Unicast`	Directs the switch to poll a specific server for SNTP time synchronization. Requires at least one server address.
`Broadcast`	Directs the switch to acquire its time synchronization from data broadcast by any SNTP server to the network broadcast address. The switch uses the first server detected and ignores any others. However, if the Poll Interval expires three times without the switch detecting a time update from

Table 2 SNTP parameters *(continued)*

SNTP parameter	Operation
	the original server, the switch accepts a broadcast time update from the next server it detects.
Poll Interval (seconds)	**In Unicast Mode:** Specifies how often the switch polls the designated SNTP server for a time update. **In Broadcast Mode:** Specifies how often the switch polls the network broadcast address for a time update. Value is between 30 to 720 seconds.
Server Address	Used only when the **SNTP Mode** is set to `Unicast`. Specifies the IP address of the SNTP server that the switch accesses for time synchronization updates. You can configure up to three servers; one using the menu or CLI, and two more using the CLI.
Server Version	Specifies the SNTP software version to use and is assigned on a per-server basis. The version setting is backwards-compatible. For example, using version 3 means that the switch accepts versions 1 through 3. Default: 3; range: 1 to 7.
Priority	Specifies the order in which the configured servers are polled for getting the time. Value is between 1 and 3.

Enabling the SNTP mode means to configure it for either broadcast or unicast mode. Remember that to run SNTP as the switch's time synchronization protocol, you must also select SNTP as the time synchronization method by using the CLI `timesync` command (or the Menu interface `Time Sync Method` parameter).

Syntax:

```
timesync sntp
```

Selects SNTP as the time protocol (“Viewing and configuring SNTP (CLI)” (page 24)).

```
sntp [  broadcast | unicast  ]
```

Enables the SNTP mode (page A-7 and “Enabling SNTP in unicast mode (CLI)” (page 27)).

Syntax:

```
sntp server  ip-addr
```

Required only for unicast mode (“Enabling SNTP in unicast mode (CLI)” (page 27)).

Syntax:

```
sntp poll-interval  [ 30 - 720 ]
```

Enabling the SNTP mode also enables the SNTP poll interval (default: 720 seconds; “Changing the SNTP poll interval (CLI)” (page 29)).

Syntax:

```
sntp server priority [1 - 3 ]
```

Specifies the order in which the configured servers are polled for getting the time (page A-11).

About SNTP unicast time polling with multiple SNTP servers

When running SNTP unicast time polling as the time synchronization method, the switch requests a time update from the server you configured with either the `Server Address` parameter in the menu interface, or the primary server in a list of up to three SNTP servers configured using the CLI. If the switch does not receive a response from the primary server after three consecutive polling intervals, the switch tries the next server (if any) in the list. If the switch tries all servers in the list without success, it sends an error message to the Event Log and reschedules to try the address list again after the configured `Poll Interval` time has expired.

If there are already three SNTP server addresses configured on the switch, and you want to use the CLI to replace one of the existing addresses with a new one, you must delete the unwanted address before you configure the new one.

About operating with multiple SNTP server addresses configured (Menu)

When you use the Menu interface to configure an SNTP server IP address, the new address writes over the current primary address, if one is configured.

About SNTP client authentication

Enabling SNTP authentication allows network devices such as HP switches to validate the SNTP messages received from an NTP or SNTP server before updating the network time. NTP or SNTP servers and clients must be configured with the same set of authentication keys so that the servers can authenticate the messages they send and clients (HP switches) can validate the received messages before updating the time.

This feature provides support for SNTP client authentication on HP switches, which addresses security considerations when deploying SNTP in a network.

Requirements

You must configure the following to enable SNTP client authentication on the switch.

SNTP client authentication support

- Timesync mode must be SNTP. Use the `timesync sntp` command. (SNTP is disabled by default).
- SNTP must be in unicast or broadcast mode. See "Configuring unicast and broadcast mode for authentication" (page 34).
- The MD5 authentication mode must be selected.
- An SNTP authentication key-identifier (`key-id`) must be configured on the switch and a value (`key-value`) must be provided for the authentication key. A maximum of 8 sets of `key-id` and `key-value` can be configured on the switch.
- Among the keys that have been configured, one key or a set of keys must be configured as trusted. Only trusted keys are used for SNTP authentication.
- If the SNTP server requires authentication, one of the trusted keys has to be associated with the SNTP server.
- SNTP client authentication must be enabled on the HP Switch. If client authentication is disabled, packets are processed without authentication.

All of the above steps are necessary to enable authentication on the client.

SNTP server authentication support

NOTE: SNTP server is not supported on HP Switch products.

You must perform the following on the SNTP server:

- The same authentication key-identifier, trusted key, authentication mode and key-value that were configured on the SNTP client must also be configured on the SNTP server.
- SNTP server authentication must be enabled on the server.

If any of the parameters on the server are changed, the parameters have to be changed on all the SNTP clients in the network as well. The authentication check fails on the clients otherwise, and the SNTP packets are dropped.

About configuring a trusted key

Trusted keys are used in SNTP authentication. In unicast mode, you must associate a `trusted` key with a specific NTP/SNTP server. That key is used for authenticating the SNTP packet.

In unicast mode, a specific server is configured on the switch so that the SNTP client communicates with the specified server to get the date and time.

In broadcast mode, the SNTP client switch checks the size of the received packet to determine if it is authenticated. If the broadcast packet is authenticated, the key-id value is checked to see if the same key-id value is configured on the SNTP client switch. If the switch is configured with the same key-id value, and the key-id value is configured as "trusted," the authentication succeeds. Only trusted key-id value information is used for SNTP authentication. For information about configuring these modes, see “Configuring unicast and broadcast mode for authentication” (page 34).

If the packet contains key-id value information that is not configured on the SNTP client switch, or if the received packet contains no authentication information, it is discarded. The SNTP client switch expects packets to be authenticated if SNTP authentication is enabled.

When authentication succeeds, the time in the packet is used to update the time on the switch.

About saving configuration files and the `include-credentials` command

You can use the `include-credentials` command to store security information in the running-config file. This allows you to upload the file to a TFTP server and then later download the file to the HP switches on which you want to use the same settings. For more information about the `include-credentials` command, see "Configuring Username and Password Security" in the *Access Security Guide* for your switch.

The authentication key values are shown in the output of the `show running-config` and `show config` commands only if the `include-credentials` command was executed.

When SNTP authentication is configured and `include-credentials` has not been executed, the SNTP authentication configuration is not saved.

Configuration file with SNTP authentication information example

```
 HP Switch (config) # show config
Startup configuration:
.
.
.
timesync sntp
sntp broadcast
sntp 50
sntp authentication
sntp server priority 1 10.10.10.2.3 key-id 55
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4 key-id 55
```

NOTE: SNTP authentication has been enabled and a key-id of 55 has been created.

In this example, the `include-credentials` command has not been executed and is not present in the configuration file. The configuration file is subsequently saved to a TFTP server for later use. The SNTP authentication information is not saved and is not present in the retreived configuration files, as shown in the following figure.

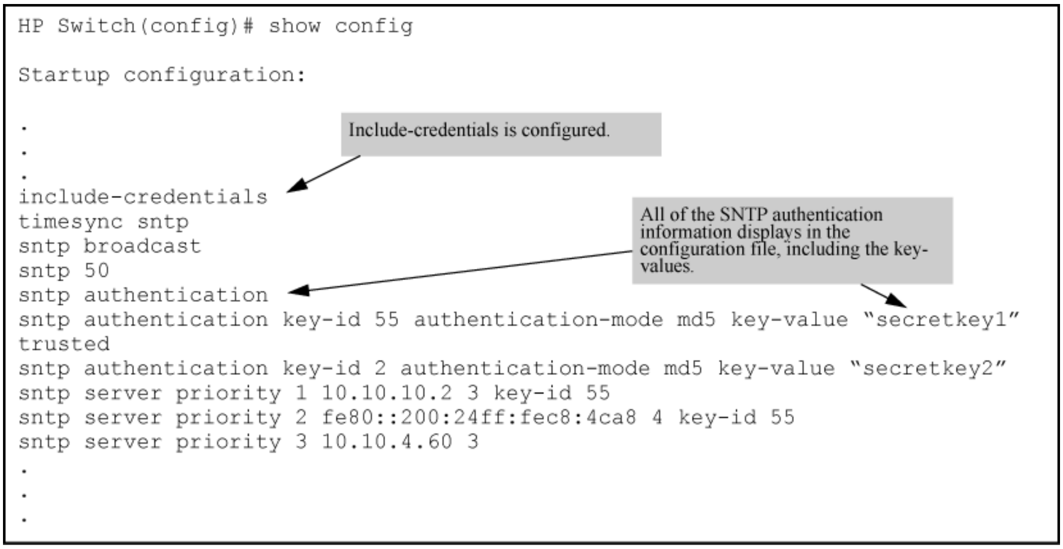
Retrieved configuration file when `include credentials` is not configured

```
HP Switch (config) # copy tftp startup-config 10.2.3.44 config1
.
.
.
Switch reboots ...
.
Startup configuration
.
.
.
timesync sntp
sntp broadcast
sntp 50 sntp server priority 1 10.10.10.2.3
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4
.
.
.
```

NOTE: The SNTP authentication line and the Key-ids are not displayed. You must reconfigure SNTP authentication.

If `include-credentials` is configured, the SNTP authentication configuration is saved in the configuration file. When the `show config` command is entered, all of the information that has been configured for SNTP authentication displays, including the key-values.

Figure 14 Saved SNTP Authentication information when `include-credentials` is configured



```
HP Switch(config)# show config

Startup configuration:

.
.
.
include-credentials
timesync sntp
sntp broadcast
sntp 50
sntp authentication
sntp authentication key-id 55 authentication-mode md5 key-value "secretkey1"
trusted
sntp authentication key-id 2 authentication-mode md5 key-value "secretkey2"
sntp server priority 1 10.10.10.2 3 key-id 55
sntp server priority 2 fe80::200:24ff:fec8:4ca8 4 key-id 55
sntp server priority 3 10.10.4.60 3
.
.
.
```

Include-credentials is configured.

All of the SNTP authentication information displays in the configuration file, including the key-values.

SNTP messages in the Event Log

If an SNTP time change of more than three seconds occurs, the switch's Event Log records the change. SNTP time changes of less than three seconds do not appear in the Event Log.

About TimeP time synchronization

You can either manually assign the switch to use a TimeP server or use DHCP to assign the TimeP server. In either case, the switch can get its time synchronization updates from only one, designated TimeP server. This option enhances security by specifying which time server to use.

About TimeP: Selecting, and configuring

Table 3 (page 50) shows TimeP parameters and their operations.

Table 3 TimeP parameters

TimeP parameter	Operation
Time Sync Method	Used to select either TIMEP (the default), SNTP, or None as the time synchronization method.
Timep Mode	
Disabled	The Default. Timep does not operate, even if specified by the Menu interface **Time Sync Method** parameter or the CLI `timesync` command.
DHCP	When Timep is selected as the time synchronization method, the switch attempts to acquire a Timep server IP address via DHCP. If the switch receives a server address, it polls the server for updates according to the Timep poll interval. If the switch does not receive a Timep server IP address, it cannot perform time synchronization updates.
Manual	When Timep is selected as the time synchronization method, the switch attempts to poll the specified server for updates according to the Timep poll interval. If the switch fails to receive updates from the server, time synchronization updates do not occur.
Server Address	Used only when the **TimeP Mode** is set to **Manual**. Specifies the IP address of the TimeP server that the switch accesses for time synchronization updates. You can configure one server.

Enabling the TimeP mode means to configure it for either broadcast or unicast mode. Remember that to run TimeP as the switch's time synchronization protocol, you must also select TimeP as the time synchronization method by using the CLI `timesync` command (or the Menu interface `Time Sync Method` parameter).

Syntax:

```
timesync timep
```

Selects TimeP as the time protocol ("Viewing the current TimeP configuration (CLI)" (page 38)).

Syntax:

```
ip timep  dhcp | manual
```

Enables the selected TimeP mode ("Configuring (Enabling or Disabling) the TimeP mode" (page 39) and "Enabling TimeP in manual mode (CLI)" (page 40)).

Syntax:

```
no ip timep
```

Disables the TimeP mode ("Disabling the TimeP mode" (page 43)).

Syntax:

```
no timesync
```

Disables the time protocol ("Disabling time synchronization without changing the TimeP configuration (CLI)" (page 42)).

3 Port Status and Configuration

Command Summary

Table 4 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
`show interfaces brief`	Lists the current operating status for all ports on the switch	-	(page 52)	-
`show interfaces config`	For each port, shows whether the port is enabled, the operating mode, and whether it is configured for flow control	-	(page 52)	-
`show interfaces status`	Displays tagged and untagged VLAN information for a port as well as port status, configuration mode, speed, and type.	-	"Displaying the port VLAN tagged status" (page 53)	-
`show interfaces display`	Initiate the dynamic update of the `show interfaces` command	-	(page 54)	(page 54)
`show interfaces custom`	Enables you to create show commands displaying the information that you want to see in any order you want	-	(page 55)	-
`show interfaces port-utilization`	Enables you to view a real-time rate display for all ports on the switch	-	(page 56)	-
`show tech transceivers`	Enables you to • Remotely identify transceiver type and revision number without having to physically remove an installed transceiver from its slot • Display real-time status information about all installed transceivers, including non-operational transceivers	-	(page 56)	-
`interface`	For configuring ports	-	(page 55)	-
`disable/enable`	Disables or enables the port for network traffic	enable	(page 55)	-
`speed-duplex`	Specifies the port's data transfer speed and mode	auto	(page 55)	-
`flow-control`	Enables or disables flow control packets on the port	disabled	(page 59)	-
`auto-mdix`	Automatically configures the port for automatic detection of the cable (either straight-through or crossover)	auto	(page 61)	-

Table 4 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`name`	Configuring friendly port names	-	(page 64)	-
`show name`	Displays friendly port names	-	(page 65)	-
`usb port`	Allows configuration of the USB port with either the CLI or SNMP	-	(page 58)	-
`port status`	Displays the configuration for ports and (if configured) any trunk groups	-	-	(page 103)
`port/trunk settings`	Configures both individual ports and port trunk groups	enabled	-	(page 64)
`module` *`module-num`* `type` *`module-type`*	Shows module type	-	(page 68)	-
`[no] module` *`slot`*	Clears a module configuration	-	(page 68)	-
`link-keepalive`	Enables UDLD on a port or range of ports	disabled	(page 68)	-
`interval`	Determines the time interval to send UDLD control packets	50 (5 seconds)	(page 68)	-
`retries`	Determines the maximum number of retries to send UDLD control packets	5	(page 68)	-
`vlan` *`vid`*	Assigns a VLAN ID to a UDLD-enabled port for sending tagged UDLD control packets	untagged	(page 68)	-
`show link-keepalive`	Displays all the ports that are enabled for `link-keepalive`	-	(page 70)	-
`statistics`	Displays detailed statistics for the UDLD-enabled ports on the switch	-	(page 70)	-
`clear link-keepalive statistics`	Clears UDLD statistics	-	(page 70)	-

Viewing port status and configuration (CLI)

Use the following commands to display port status and configuration data.

Syntax:

`show interfaces [ brief | config |` *`port-list`* `]`

`brief` Lists the current operating status for all ports on the switch.

`config` Lists a subset of configuration data for all ports on the switch; that is, for each port, the display shows whether the port is enabled, the operating mode, and whether it is configured for flow control.

`port-list` Shows a summary of network traffic handled by the specified ports.

Examples

Example 17 `show interfaces brief` command listing

```
HP Switch(config)# show interfaces brief
Status and Counters - Port Status

                | Intrusion                           MDI   Flow  Bcast
Port  Type      | Alert     Enabled Status Mode       Mode  Ctrl  Limit
----- --------- + --------- ------- ------ ---------- ----- ----- ------
B1    100/1000T | No        Yes     Down   Auto-10-100 Auto  off   0
B2    100/1000T | No        Yes     Down   1000FDx    Auto  off   0
B3    100/1000T | No        Yes     Down   1000FDx    Auto  off   0
B4    100/1000T | No        Yes     Down   1000FDx    Auto  off   0
B5    100/1000T | No        Yes     Down   1000FDx    Auto  off   0
B6    100/1000T | No        Yes     Down   1000FDx    Auto  off   0
```

Example 18 `show interfaces config` command listing

```
HP Switch(config)# show interfaces config

 Port Settings


  Port  Type      | Enabled Mode         Flow Ctrl MDI
  ----- --------- + ------- ------------ --------- ----
  B1    100/1000T | Yes     Auto-10-100  Disable   Auto
  B2    100/1000T | Yes     Auto         Disable   Auto
  B3    100/1000T | Yes     Auto         Disable   Auto
  B4    100/1000T | Yes     Auto         Disable   Auto
  B5    100/1000T | Yes     Auto         Disable   Auto
  B6    100/1000T | Yes     Auto         Disable   Auto
```

Displaying the port VLAN tagged status

The `show interfaces status` command displays port status, configuration mode, speed, type and tagged or untagged information.

Tagged values can be:

- VLAN ID: When the VLAN number is displayed, the port is a member of a single tagged VLAN.
- multi: When "multi" is displayed, the port is a member of multiple tagged VLANs.
- no: When "no" is displayed, the port is not a member of any tagged VLAN.

Untagged values can be:

- VLAN-ID: When the VLAN number is displayed, the port is a member of a single untagged VLAN.
- multi: When "multi" is displayed, the port is added to multiple untagged VLANs.
- no: When "no" is displayed, the port is not a member of any tagged VLAN.

If the port is part of a trunk, then the trunk_VLAN membership is display in the Tagged and Untagged columns.

Example

```
HP-Switch(config)# show interfaces status
Port Name Status Config-mode Speed Type Tagged Untagged
-------- -------- ------ ----------- ------- --------- ------ ---------
```

```
A1 Up Auto 1000FDx 100/1000T 2 1
A2 Down 10HDx 10HDx 100/1000T multi 2
A3 Down 100HDx 100HDx 100/1000T multi 3
A4 Down 10FDx 10FDx 100/1000T 5 4
A5-Trk1 Down 100FDx 100FDx 100/1000T No No
A6 Down Auto 1000FDx 100/1000T No 6
A7 Down Auto-10 10HDx 100/1000T No 7
```

Dynamically updating the show interfaces command (CLI/Menu)

Syntax:

```
show interfaces display
```

Uses the `display` option to initiate the dynamic update of the `show interfaces` command, with the output being the same as the `show interfaces` command.

NOTE: Select **Back** to exit the display.

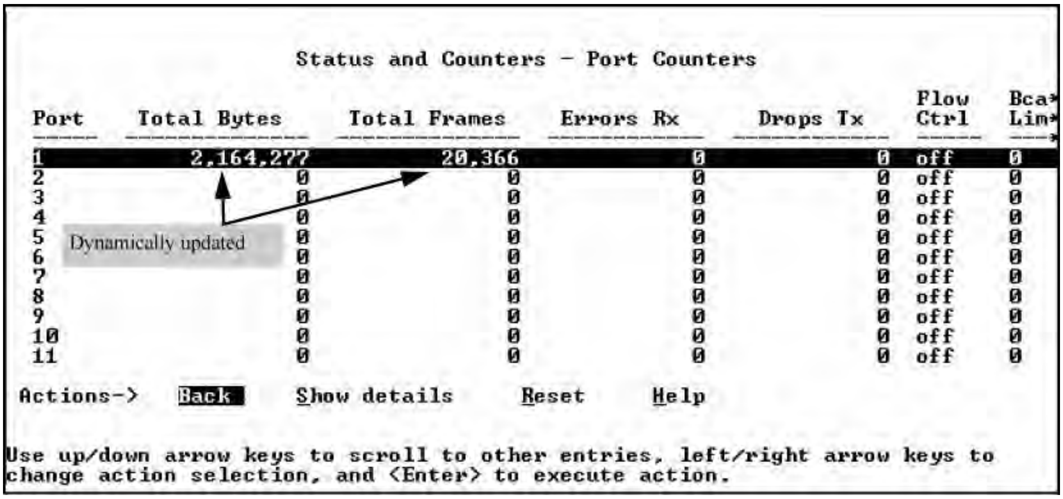
Example

```
HP Switch# show interfaces display
```

When using the **display** option in the CLI, the information stays on the screen and is updated every 3 seconds, as occurs with the display using the menu feature. The update is terminated with **Cntl-C**.

You can use the arrow keys to scroll through the screen when the output does not fit in one screen.

Figure 15 `show interfaces display` command with dynamically updating output



```
                    Status and Counters - Port Counters

                                                                      Flow   Bca*
 Port     Total Bytes     Total Frames     Errors Rx       Drops Tx     Ctrl   Lim*
 ------   --------------  --------------   ------------   ------------  ------ ---*
 1             2,164,277          20,366              0              0  off    0
 2                     0               0              0              0  off    0
 3                     0               0              0              0  off    0
 4                     0               0              0              0  off    0
 5                     0               0              0              0  off    0
 6                     0               0              0              0  off    0
 7                     0               0              0              0  off    0
 8                     0               0              0              0  off    0
 9                     0               0              0              0  off    0
 10                    0               0              0              0  off    0
 11                    0               0              0              0  off    0

Actions->   Back     Show details     Reset     Help

Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Dynamically updated

Customizing the show interfaces command (CLI)

You can create `show` commands displaying the information that you want to see in any order you want by using the `custom` option.

Syntax:

`show interfaces custom` [`port-list`] *`column-list`*

Select the information that you want to display. Supported columns are shown in Table 5 (page 55).

Table 5 Supported columns, what they display, and examples

Parameter column	Displays	Examples
port	Port identifier	A2
type	Port type	100/1000T
status	Port status	up or down
speed	Connection speed and duplex	1000FDX
mode	Configured mode	auto, auto-100, 100FDX
mdi	MDI mode	auto, MDIX
flow	Flow control	on or off
name	Friendly port name	
vlanid	The vlan id this port belongs to, or "tagged" if it belongs to more than one vlan	4 tagged
enabled	port is or is not enabled	yes or no intrusion
intrusion	Intrusion alert status	no
bcast	Broadcast limit	0

Example 19 Example of the custom `show interfaces` command

```
HP Switch(config)# show int custom 1-4 port name:4 type vlan intrusion speed enabled mdi

 Status and Counters - Custom Port Status

                                   Intrusion
  Port Name       Type       VLAN  Alert     Speed   Enabled MDI-mode
  ---- ---------- ---------- ----- --------- ------- ------- --------
  1    Acco       100/1000T  1     No        1000FDx Yes     Auto
  2    Huma       100/1000T  1     No        1000FDx Yes     Auto
  3    Deve       100/1000T  1     No        1000FDx Yes     Auto
  4    Lab1       100/1000T  1     No        1000FDx Yes     Auto
```

You can specify the column width by entering a colon after the column name, then indicating the number of characters to display. In Example 19 (page 55), the Name column displays only the first four characters of the name. All remaining characters are truncated.

NOTE: Each field has a fixed minimum width to be displayed. If you specify a field width smaller than the minimum width, the information is displayed at the minimum width. For example, if the minimum width for the Name field is 4 characters and you specify Name:2, the Name field displays 4 characters.

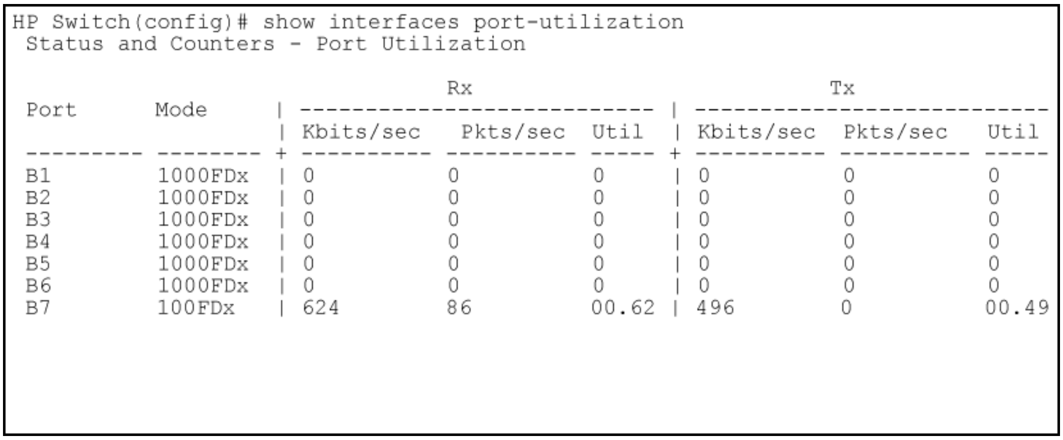
You can enter parameters in any order. There is a limit of 80 characters per line; if you exceed this limit an error displays.

For information on error messages associated with this command and for notes about pattern matching with this command, see Error messages associated with the show interfaces command (page 74).

Viewing port utilization statistics (CLI)

Use the `show interface port-utilization` command to view a real-time rate display for all ports on the switch. Figure 16 (page 56) shows a sample output from this command.

Figure 16 Example of a `show interface port-utilization` command listing



```
HP Switch(config)# show interfaces port-utilization
 Status and Counters - Port Utilization

                                    Rx                           Tx
 Port      Mode     | --------------------------- | ---------------------------
                    | Kbits/sec   Pkts/sec  Util  | Kbits/sec  Pkts/sec   Util
 --------- -------- + ---------- ---------- ----- + ---------- ---------- -----
 B1        1000FDx  | 0          0          0     | 0          0          0
 B2        1000FDx  | 0          0          0     | 0          0          0
 B3        1000FDx  | 0          0          0     | 0          0          0
 B4        1000FDx  | 0          0          0     | 0          0          0
 B5        1000FDx  | 0          0          0     | 0          0          0
 B6        1000FDx  | 0          0          0     | 0          0          0
 B7        100FDx   | 624        86         00.62 | 496        0          00.49
```

Operating notes for viewing port utilization statistics

- For each port on the switch, the command provides a real-time display of the rate at which data is received (Rx) and transmitted (Tx) in terms of kilobits per second (KBits/s), number of packets per second (Pkts/s), and utilization (Util) expressed as a percentage of the total bandwidth available.
- The `show interfaces` *`port-list`* command can be used to display the current link status and the port rate average over a 5 minute period. Port rates are shown in bits per second (bps) for ports up to 1 Gigabit; for 10 Gigabit ports, port rates are shown in kilobits per second (Kbps).

Viewing transceiver status (CLI)

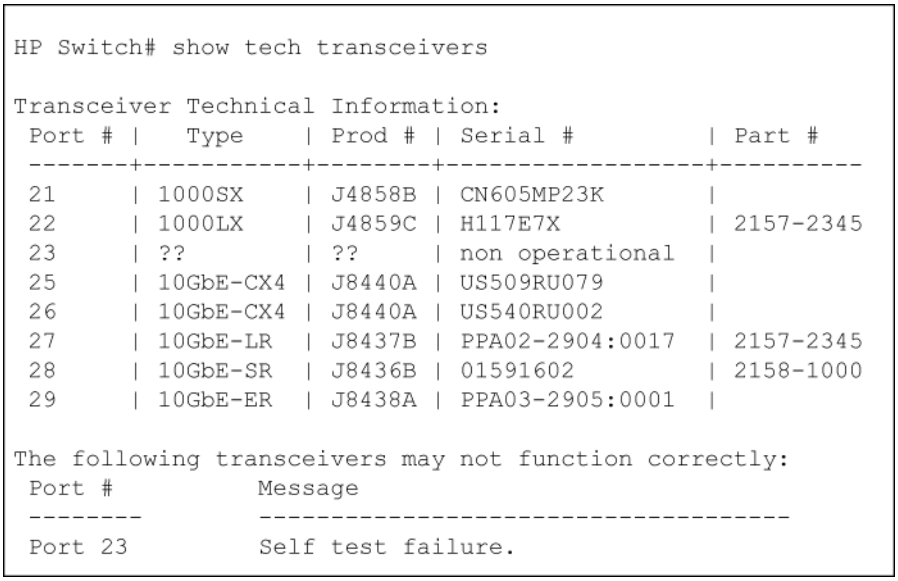
The `show interfaces transceivers` command allows you to:

- Remotely identify transceiver type and revision number without having to physically remove an installed transceiver from its slot.
- Display real-timestatus information about all installed transceivers, including non-operational transceivers.

Figure 17 (page 57) shows sample output from the `show tech transceivers` command.

NOTE: Part # column in Figure 17 (page 57) enables you to determine the manufacturer for a specified transceiver and revision number.

Figure 17 Example of `show tech transceivers` command



```
HP Switch# show tech transceivers

Transceiver Technical Information:
 Port # |   Type     | Prod # | Serial #           | Part #
 -------+------------+--------+--------------------+----------
 21     | 1000SX     | J4858B | CN605MP23K         |
 22     | 1000LX     | J4859C | H117E7X            | 2157-2345
 23     | ??         | ??     | non operational    |
 25     | 10GbE-CX4  | J8440A | US509RU079         |
 26     | 10GbE-CX4  | J8440A | US540RU002         |
 27     | 10GbE-LR   | J8437B | PPA02-2904:0017    | 2157-2345
 28     | 10GbE-SR   | J8436B | 01591602           | 2158-1000
 29     | 10GbE-ER   | J8438A | PPA03-2905:0001    |

The following transceivers may not function correctly:
 Port #         Message
 --------       -------------------------------------
 Port 23        Self test failure.
```

Operating notes

- The following information is displayed for each installed transceiver:
  - Port number on which transceiver is installed.
  - Type of transceiver.
  - Product number — Includes revision letter, such as A, B, or C. If no revision letter follows a product number, this means that no revision is available for the transceiver.
  - Part number — Allows you to determine the manufacturer for a specified transceiver and revision number.
- For a non-HP switches installed transceiver (see line 23 Figure 17 (page 57)), no transceiver type, product number, or part information is displayed. In the Serial Number field, `non-operational` is displayed instead of a serial number.
- The following error messages may be displayed for a non-operational transceiver:
  - `Unsupported Transceiver. (SelfTest Err#060)`
    `Check: www.hp.com/rnd/device_help/2_inform for more info.`
  - `This switch only supports revision B and above transceivers.`
    `Check: www.hp.com/rnd/device_help/2_inform for more info.`
  - `Self test failure.`
  - `Transceiver type not supported in this port.`
  - `Transceiver type not supported in this software version.`
  - `Not an HP Switch Transceiver.`
    `Go to: www.hp.com/rnd/device_help/2_inform for more info.`

Enabling or disabling ports and configuring port mode (CLI)

You can configure one or more of the following port parameters. See Table 6 (page 72) (Broadcast limit (page 74)).

Syntax:

`interface` *`port-list`* `[ disable | enable ]`

Disables or enables the port for network traffic. Does not use the no form of the command. (Default: `enable`.)

`speed-duplex [ auto-10 | 10-full | 10-half | 100-full | 100-half | auto | auto-100 | 1000-full ]`

Note that in the above syntax, you can substitute `int` for `interface` (for example, `int` *`port-list`*).

Specifies the port's data transfer speed and mode. Does not use the no form of the command. (Default: `auto`.)

The 10/100 auto-negotiation feature allows a port to establish a link with a port at the other end at either 10 Mbps or 100 Mbps, using the highest mutual speed and duplex mode available. Only these speeds are allowed with this setting.

Examples

To configure port C5 for auto-10-100, enter this command:

```
HP Switch(config)# int c5 speed-duplex auto-10-100
```

To configure ports C1 through C3 and port C6 for 100Mbps full-duplex, enter these commands:

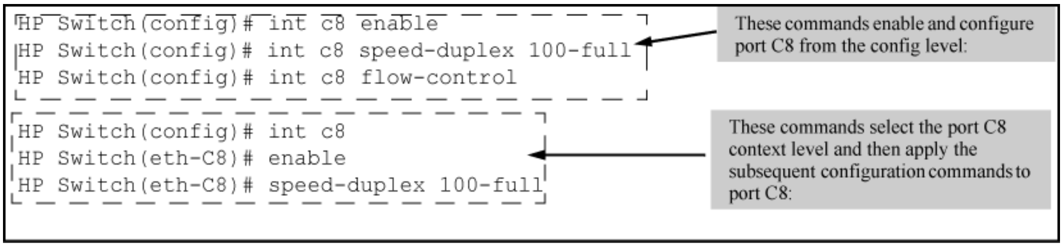
```
HP Switch(config)# int c1-c3,c6 speed-duplex 100-full
```

Similarly, to configure a single port with the above command settings, you could either enter the same command with only the one port identified or go to the context level for that port and then enter the command. For example, to enter the context level for port C6 and then configure that port for 100FDx:

```
HP Switch(config)# int e c6
HP Switch(eth-C6)# speed-duplex 100-full
```

If port C8 was disabled, and you wanted to enable it and configure it for 100FDx with flow-control active, you could do so with either of the following command sets:

Figure 18 Two methods for changing a port configuration



```
HP Switch(config)# int c8 enable
HP Switch(config)# int c8 speed-duplex 100-full
HP Switch(config)# int c8 flow-control
```

These commands enable and configure port C8 from the config level:

```
HP Switch(config)# int c8
HP Switch(eth-C8)# enable
HP Switch(eth-C8)# speed-duplex 100-full
```

These commands select the port C8 context level and then apply the subsequent configuration commands to port C8:

For more on flow control, see "Enabling or disabling flow control (CLI)" (page 59).

Enabling or disabling the USB port (CLI/SNMP)

This feature allows configuration of the USB port with either the CLI or SNMP.

To enable/disable the USB port with the CLI:

Syntax:

```
usb-port
no usb-port
```

Enables the USB port. The no form of the command disables the USB port and any access to the device.

To display the status of the USB port:

Syntax:

`show usb-port`

Displays the status of the USB port. It can be enabled, disabled, or not present.

Figure 19 Example of `show usb-port` command output on version K.13.59 and later

```
HP Switch(config)# show usb-port

  USB port status: enabled
  USB port power status: power on (USB device detected in port)
  USB port reseat status: USB reseat not required
```

Figure 20 Example of `show usb-port` command output on version K.14.XX

```
HP Switch(config)# show usb-port

  USB port status: enabled
  USB port power status: power on    (USB device detected in port)
```

One of the following messages indicates the presence or absence of the USB device:

- Not able to sense device in USB port
- USB device detected in port
- no USB device detected in port

The reseat status messages can be one of the following (K.13.XX only):

- undetermined USB reseat requirement
- USB reseat not required
- USB device reseat required for USB autorun

The autorun feature works only when a USB device is inserted and the USB port is enabled..

Software versions K.13.XX operation

When using software version K.13.58, if the USB port is disabled (no usb-port command), the USB autorun function does not work in the USB port until the USB port is enabled, the config file is saved, and the switch is rebooted. The 5 volt power to the USB port remains on even after the USB port has been disabled. For software versions after K.13.58, the 5 volt power applied to the USB port is synchronized with the enabling of the USB port, that is, when the USB port is enabled, the 5 volts are supplied; when the USB port is disabled, the 5 volts are not supplied. For previous software versions the power was supplied continuously. The autorun function does not require a switch reboot, but the USB device must be inserted at least once after the port is enabled so that the switch recognizes that the device is present. If the USB device is inserted and then the USB port is enabled, the switch does not recognize that a USB device is present.

Software Version K.14.XX Operation.

For software versions K.14.XX, the USB port can be disabled and enabled without affecting the autorun feature. When the USB port is enabled, the autorun feature activates if a USB device is already inserted in the USB port. Power is synchronized with the enabling and disabling of USB ports as described above for K.13.59 and later software.

Enabling or disabling flow control (CLI)

NOTE: You must enable flow control on both ports in a given link. Otherwise, flow control does not operate on the link and appears as `Off` in the `show interfaces brief` port listing, even if flow control is configured as enabled on the port in the switch. (See Example 17 (page 53).) Also, the port (speed-duplex) mode must be set to `Auto` (the default).

To disable flow control on some ports, while leaving it enabled on other ports, just disable it on the individual ports you want to exclude. (You can find more information on flow control in Table 6 (page 72).)

Syntax:

```
[no] interface  port-list  flow-control
```

Enables or disables flow control packets on the port. The `no` form of the command disables flow control on the individual ports. (Default: Disabled.)

Examples

Suppose that:

1. You want to enable flow control on ports A1-A6.
2. Later, you decide to disable flow control on ports A5 and A6.
3. As a final step, you want to disable flow control on all ports.

Assuming that flow control is currently disabled on the switch, you would use these commands:

Example 20 Configuring flow control for a series of ports

```
HP Switch(config)# int a1-a6 flow-control
HP Switch(config)# show interfaces brief

 Status and Counters - Port Status

                   | Intrusion                           MDI  Flow Bcast
  Port   Type      | Alert     Enabled Status Mode       Mode Ctrl Limit
  ------ --------- + --------- ------- ------ ---------- ---- ---- -----
  A1     10GbE-T   | No        Yes     Up     1000FDx    NA   on   0
  A2     10GbE-T   | No        Yes     Up     10GigFD    NA   on   0
  A3     10GbE-T   | No        Yes     Up     10GigFD    NA   on   0
  A4     10GbE-T   | No        Yes     Up     10GigFD    NA   on   0
  A5     10GbE-T   | No        Yes     Up     10GigFD    NA   on   0
  A6     10GbE-T   | No        Yes     Up     10GigFD    NA   on   0
  A7     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A8     10GbE-T   | No        Yes     Up     10GigFD    NA   off  0
```

Example 21 Example continued from Example 20 (page 61)

```
HP Switch(config)# no int a5-a6 flow-control
HP Switch(config)# show interfaces brief

 Status and Counters - Port Status

                   | Intrusion                           MDI  Flow Bcast
  Port   Type      | Alert     Enabled Status Mode       Mode Ctrl Limit
  ------ --------- + --------- ------- ------ ---------- ---- ---- -----
  A1     10GbE-T   | No        Yes     Up     1000FDx    NA   on   0
  A2     10GbE-T   | No        Yes     Down   10GigFD    NA   on   0
  A3     10GbE-T   | No        Yes     Down   10GigFD    NA   on   0
  A4     10GbE-T   | No        Yes     Down   10GigFD    NA   on   0
  A5     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A6     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A7     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A8     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
```

Example 22 Example continued from Example 21 (page 61)

```
HP Switch(config)# no int a1-a4 flow-control
HP Switch(config)# show interfaces brief

 Status and Counters - Port Status

                   | Intrusion                           MDI  Flow Bcast
  Port   Type      | Alert     Enabled Status Mode       Mode Ctrl Limit
  ------ --------- + --------- ------- ------ ---------- ---- ---- -----
  A1     10GbE-T   | No        Yes     Down   1000FDx    NA   off  0
  A2     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A3     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A4     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A5     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A6     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A7     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
  A8     10GbE-T   | No        Yes     Down   10GigFD    NA   off  0
```

Configuring auto-MDIX (CLI)

The auto-MDIX features apply only to copper port switches using twisted-pair copper Ethernet cables. For information about auto-MDIX, see "About configuring auto-MDIX" (page 74).

Syntax:

```
interface  port-list  mdix-mode[  auto-mdix | mdi | mdix  ]
```

`auto-mdix`	The automatic,default setting. This configures the port for automatic detection of the cable (either straight-through or crossover).
`mdi`	The manual mode setting that configures the port for connecting to either a PC or other MDI device with a crossover cable, or to a switch, hub, or other MDI-X device with a straight-through cable.
`mdix`	The manual mode setting that configures the port for connecting to either a switch, hub, or other MDI-X device with a crossover cable, or to a PC or other MDI device with a straight-through cable.

Syntax:

```
show interfaces config
```

Lists the current per-port Auto/MDI/MDI-X configuration.

Syntax:

```
show interfaces brief
```

- Where a port is linked to another device, this command lists the MDI mode the port is currently using.
- In the case of ports configured for `Auto` (`auto-mdix`), the MDI mode appears as either `MDI` or `MDIX`, depending upon which option the port has negotiated with the device on the other end of the link.
- In the case of ports configured for `MDI` or `MDIX`, the mode listed in this display matches the configured setting.
- If the link to another device was up, but has gone down, this command shows the last operating MDI mode the port was using.
- If a port on a given switch has not detected a link to another device since the last reboot, this command lists the MDI mode to which the port is currently configured.

Example

`show interfaces config` displays the following data when port A1 is configured for `auto-mdix`, port A2 is configured for `mdi`, and port A3 is configured for `mdix`:

Example 23 Example of displaying the current MDI configuration

```
HP Switch(config)# show interfaces config

 Port Settings

  Port   Type      | Enabled Mode         Flow Ctrl MDI
  ------ --------- + ------- ------------ --------- ----
  A1     10GbE-T   | Yes     Auto         Disable   Auto
  A2     10GbE-T   | Yes     Auto         Disable   MDI
  A3     10GbE-T   | Yes     Auto         Disable   MDIX
  A4     10GbE-T   | Yes     Auto         Disable   Auto
  A5     10GbE-T   | Yes     Auto         Disable   Auto
  A6     10GbE-T   | Yes     Auto         Disable   Auto
  A7     10GbE-T   | Yes     Auto         Disable   Auto
  A8     10GbE-T   | Yes     Auto         Disable   Auto
```

Example 24 Example of displaying the current MDI operating mode

```
HP Switch(config)# show interfaces brief

 Status and Counters - Port Status

                   | Intrusion                           MDI  Flow Bcast
  Port   Type      | Alert     Enabled Status Mode       Mode Ctrl Limit
  ------ --------- + --------- ------- ------ ---------- ---- ---- -----
  A1     10GbE-T   | No        Yes     Up     1000FDx    MDIX off  0
  A2     10GbE-T   | No        Yes     Down   10GigFD    MDI  off  0
  A3     10GbE-T   | No        Yes     Down   10GigFD    MDIX off  0
  A4     10GbE-T   | No        Yes     Down   10GigFD    Auto off  0
  A5     10GbE-T   | No        Yes     Down   10GigFD    Auto off  0
  A6     10GbE-T   | No        Yes     Down   10GigFD    Auto off  0
  A7     10GbE-T   | No        Yes     Down   10GigFD    Auto off  0
  A8     10GbE-T   | No        Yes     Down   10GigFD    Auto off  0
```

Viewing port configuration (Menu)

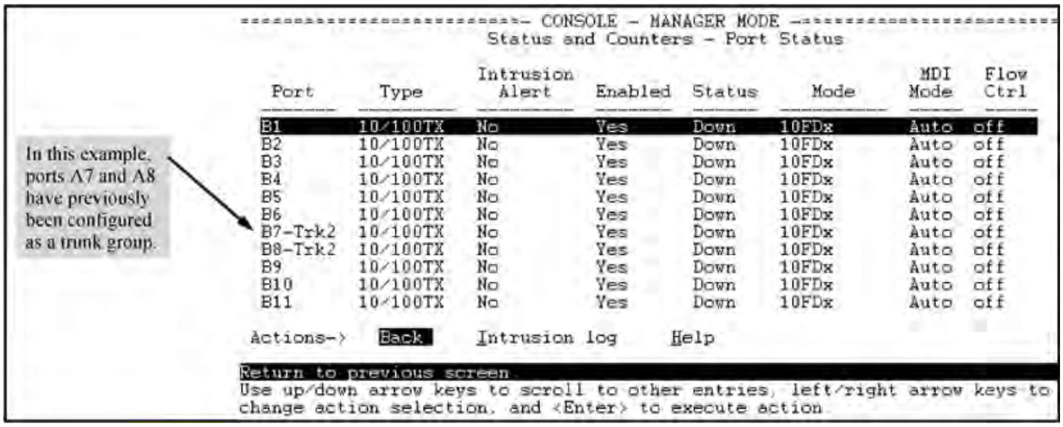
The menu interface displays the configuration for ports and (if configured) any trunk groups.

From the Main Menu, select:

1. Status and Counters

4. Port Status

Figure 21 Example of a switch port status screen



```
=========================- CONSOLE - MANAGER MODE -=========================
                     Status and Counters - Port Status

                      Intrusion                                  MDI   Flow
  Port      Type       Alert     Enabled  Status      Mode       Mode  Ctrl
  -------   --------- ---------  -------  ------  -----------   ----  -----
  B1        10/100TX  No         Yes      Down    10FDx         Auto  off
  B2        10/100TX  No         Yes      Down    10FDx         Auto  off
  B3        10/100TX  No         Yes      Down    10FDx         Auto  off
  B4        10/100TX  No         Yes      Down    10FDx         Auto  off
  B5        10/100TX  No         Yes      Down    10FDx         Auto  off
  B6        10/100TX  No         Yes      Down    10FDx         Auto  off
  B7-Trk2   10/100TX  No         Yes      Down    10FDx         Auto  off
  B8-Trk2   10/100TX  No         Yes      Down    10FDx         Auto  off
  B9        10/100TX  No         Yes      Down    10FDx         Auto  off
  B10       10/100TX  No         Yes      Down    10FDx         Auto  off
  B11       10/100TX  No         Yes      Down    10FDx         Auto  off

 Actions->   Back     Intrusion log     Help

Return to previous screen
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action
```

In this example, ports A7 and A8 have previously been configured as a trunk group.

Configuring ports (Menu)

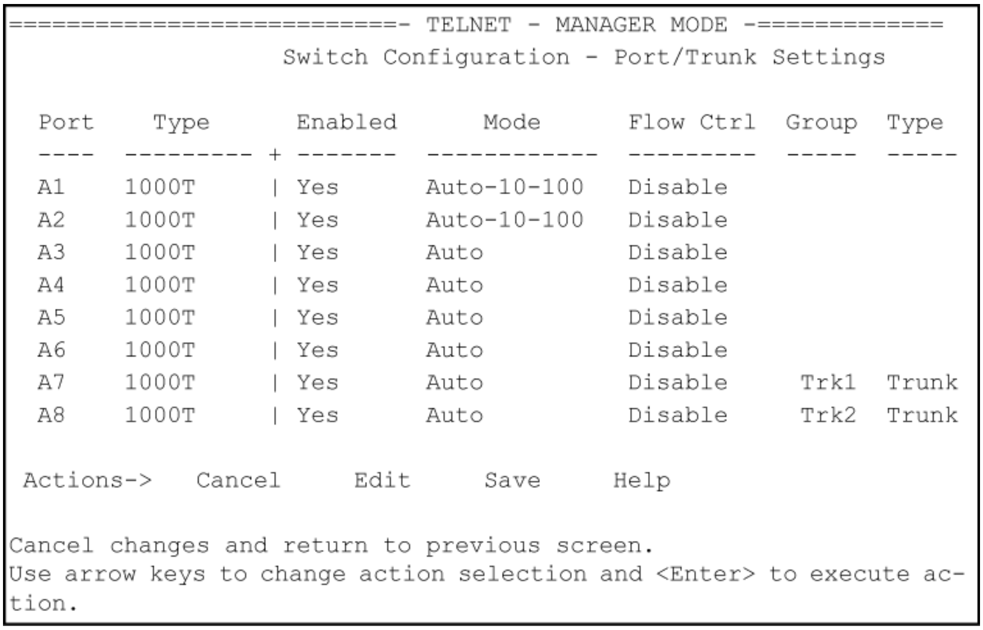
The menu interface uses the same screen for configuring both individual ports and port trunk groups. For information on port trunk groups, see Chapter 12, "Port Trunking".

1. From the Main Menu, select:

   2. Switch Configuration…

   2. Port/Trunk Settings

   Figure 22 Example of port/trunk settings with a trunk group configured



```
===========================- TELNET - MANAGER MODE -=============
                  Switch Configuration - Port/Trunk Settings

  Port    Type        Enabled      Mode         Flow Ctrl  Group  Type
  ----  --------- + -------  ------------  ---------  -----  -----
  A1    1000T     | Yes      Auto-10-100   Disable
  A2    1000T     | Yes      Auto-10-100   Disable
  A3    1000T     | Yes      Auto          Disable
  A4    1000T     | Yes      Auto          Disable
  A5    1000T     | Yes      Auto          Disable
  A6    1000T     | Yes      Auto          Disable
  A7    1000T     | Yes      Auto          Disable     Trk1   Trunk
  A8    1000T     | Yes      Auto          Disable     Trk2   Trunk

 Actions->   Cancel     Edit     Save     Help

Cancel changes and return to previous screen.
Use arrow keys to change action selection and <Enter> to execute ac-
tion.
```

2. Press `[E]` (for Edit).

   The cursor moves to the `Enabled` field for the first port.

   For further information on configuration options for these features, see the online help provided with this screen.

3. When you have finished making changes to the above parameters, press `[Enter]`, then press `[S]` (for `Save`).

Configuring friendly port names (CLI)

For detailed information about friendly port names, see "About using friendly (optional) port names" (page 75).

Syntax:

`interface` *`port-list`* `name` *`port-name-string`*

Assigns a port name to port-list.

Syntax:

`no interface` *`port-list`* `name`

Deletes the port name from `port-list`.

Configuring a single port name (CLI)

Example

Suppose that you have connected port A3 on the switch to Bill Smith's workstation, and want to assign Bill's name and workstation IP address (10.25.101.73) as a port name for port A3:

Example 25 Example of configuring a friendly port name

```
HP Switch(config)# int A3 name Bill_Smith@10.25.101.73
HP Switch(config)# write mem
HP Switch(config)# show name A3

 Port Names
  Port : A3
   Type : 10/100TX
   Name : Bill_Smith@10.25.101.73
```

Configuring the same name for multiple ports (CLI)

Example

Suppose that you want to use ports A5 through A8 as a trunked link to a server used by a drafting group. In this case you might configure ports A5 through A8 with the name "Draft-Server:Trunk."

Example 26 Example of configuring one friendly port name on multiple ports

```
HP Switch(config)# int a5-a8 name Draft-Server:Trunk
HP Switch(config)# write mem
HP Switch(config)# show name a5-a8

 Port Names

  Port : A5
   Type : 10GbE-T
   Name : Draft-Server:Trunk
 Port : A6
   Type : 10GbE-T
   Name : Draft-Server:Trunk
 Port : A7
   Type : 10GbE-T
   Name : Draft-Server:Trunk
 Port : A8
   Type : 10GbE-T
   Name : Draft-Server:Trunk
```

Displaying friendly port names with other port data (CLI)

Syntax:

`show name`

Displays a listing of port numbers with their corresponding friendly port names and also quickly shows you which ports do not have friendly name assignments. (`show name` data comes from the running-config file.)

Syntax:

`show interface` *`port-number`*

Displays the friendly port name, if any, along with the traffic statistics for that port. (The friendly port name data comes from the running-config file.)

Syntax:

`show config`

Includes friendly port names in the per-port data of the resulting configuration listing. (`show config` data comes from the startup-config file.)

Listing all ports or selected ports with their friendly port names (CLI)

Syntax:

`show name [ port-list ]`

Lists the friendly port name with its corresponding port number and port type. The `show name` command without a port list shows this data for all ports on the switch.

Example

Example 27 Example of friendly port name data for all ports on the switch

```
HP Switch(config)# show name
Port Names

  Port   Type      Name
  ------ --------- -----------------------------------------------------------
  A1     10GbE-T
  A2     10GbE-T
  A3     10GbE-T   Bill_Smith@10.25.101.73
  A4     10GbE-T
  A5     10GbE-T   Draft-Server:Trunk
  A6     10GbE-T   Draft-Server:Trunk
  A7     10GbE-T   Draft-Server:Trunk
  A8     10GbE-T   Draft-Server:Trunk
```

Example 28 Example of friendly port name data for specific ports on the switch

```
HP Switch(config)# show name A3-A5

 Port Names

  Port : A3
  Type : 10GbE-T
  Name : Bill_Smith@10.25.101.73
 Port : A4
  Type : 10GbE-T
  Name :
 Port : A5
  Type : 10GbE-T
  Name : Draft-Server:Trunk
```

Including friendly port names in per-port statistics listings (CLI)

Syntax:

`show interface` *`port-number`*

Includes the friendly port name with the port's traffic statistics listing. A friendly port name configured to a port is automatically included when you display the port's statistics output.

Example

If you configure port A1 with the name "O'Connor_10.25.101.43," the `show interface` output for this port appears similar to the following:

Example 29 Example of a friendly port name in a per-port statistics listing

```
HP Switch(config)# show interface a1

 Status and Counters - Port Counters for port A1

  Name  : O’Connor@10.25.101.43
  MAC Address     : 001871-b995ff
  Link Status     : Up
  Totals (Since boot or last clear) :
   Bytes Rx       : 2,763,197          Bytes Tx       : 22,972
   Unicast Rx     : 2044               Unicast Tx     : 128
   Bcast/Mcast Rx  : 23,456            Bcast/Mcast Tx : 26
  Errors (Since boot or last clear) :
   FCS Rx         : 0                  Drops Tx       : 0
   Alignment Rx    : 0                 Collisions Tx  : 0
   Runts Rx       : 0                  Late Colln Tx  : 0
   Giants Rx      : 0                  Excessive Colln : 0
   Total Rx Errors : 0                 Deferred Tx    : 0
  Others (Since boot or last clear) :
   Discard Rx     : 0                  Out Queue Len  : 0
   Unknown Protos  : 0
  Rates (5 minute weighted average) :
   Total Rx (bps) : 3,028,168          Total Tx  (bps) : 1,918,384
   Unicast Rx (Pkts/sec) : 5           Unicast Tx (Pkts/sec) : 0
   B/Mcast Rx (Pkts/sec) : 71          B/Mcast Tx (Pkts/sec) : 0
   Utilization Rx  : 00.30 %           Utilization Tx : 00.19 %
```

For a given port, if a friendly port name does not exist in the running-config file, the Name line in the above command output appears as:

```
Name : not assigned
```

Searching the configuration for ports with friendly port names (CLI)

This option tells you which friendly port names have been saved to the startup-config file. (`show config` does not include ports that have only default settings in the startup-config file.)

Syntax:

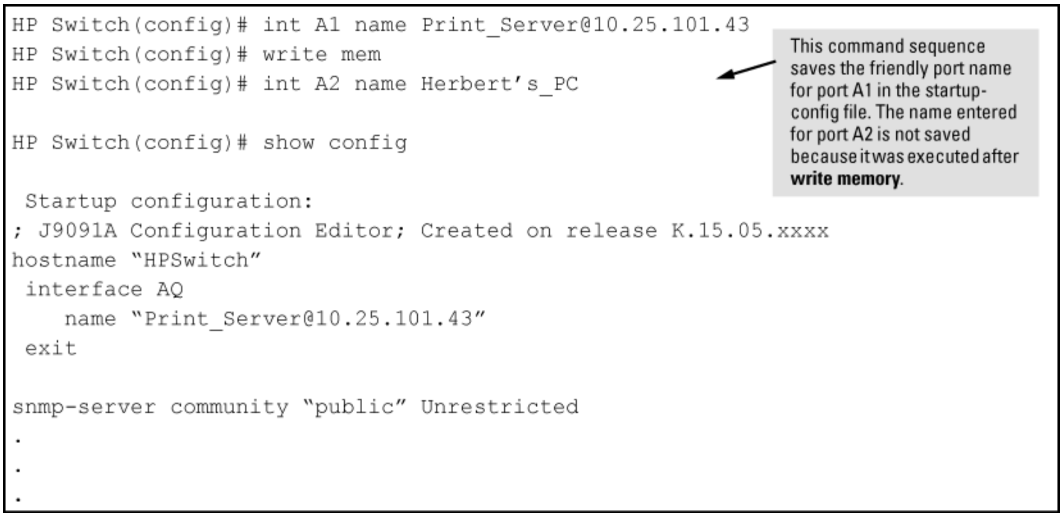
```
show config
```

Includes friendly port names in a listing of all interfaces (ports) configured with non-default settings. Excludes ports that have neither a friendly port name nor any other non-default configuration settings.

Example

If you configure port A1 with a friendly port name:

Figure 23 Example listing of the startup-config file with a friendly port name configured (and saved)



```
HP Switch(config)# int A1 name Print_Server@10.25.101.43
HP Switch(config)# write mem
HP Switch(config)# int A2 name Herbert's_PC

HP Switch(config)# show config

 Startup configuration:
; J9091A Configuration Editor; Created on release K.15.05.xxxx
hostname "HPSwitch"
 interface AQ
    name "Print_Server@10.25.101.43"
 exit

snmp-server community "public" Unrestricted
.
.
.
```

This command sequence saves the friendly port name for port A1 in the startup-config file. The name entered for port A2 is not saved because it was executed after **write memory**.

Configuring the type of a module

For detailed information about configuring transceivers and modules, see“About configuring transceivers and modules that have not been inserted” (page 76).

Syntax:

`module` *`module-num`* `type` *`module-type`*

Allows you to configure the type of the module.

Clearing the module configuration

For information about clearing module configuration and operational restrictions, see “About clearing the module configuration” (page 76).

Syntax:

[no] `module` *`slot`*

Allows removal of the module configuration in the configuration file after the module has been removed. Enter an integer between 1 and 12 for *`slot`*.

Example

```
HP Switch(config)# no module 3
```

Configuring uni-directional link detection (UDLD) (CLI)

For detailed information about UDLD, see “Uni-directional link detection (UDLD)” (page 77).

Syntax:

[no]`interface` *`port-list`* `link-keepalive`

Enables UDLD on a port or range of ports.

To disable this feature, enter the `no` form of the command.

Default: UDLD disabled

Syntax:

`link-keepalive interval` *`interval`*

Determines the time interval to send UDLD control packets. The *interval* parameter specifies how often the ports send a UDLD packet. You can specify from 10 to 100, in 100-ms increments, where 10 is 1 second, 11 is 1.1 seconds, and so on.

Default: 50 (5 seconds)

Syntax:

```
link-keepalive retries num
```

Determines the maximum number of retries to send UDLD control packets. The num parameter specifies the maximum number of times the port will try the health check. You can specify a value from 3 to 10.

Default: 5

Syntax:

```
[ no ]interface port-list link-keepalive vlan vid
```

Assigns a VLAN ID to a UDLD-enabled port for sending tagged UDLD control packets.Under default settings, untagged UDLD packets can still be transmitted and received on tagged only ports; however, a warning message is logged.

The no form of the command disables UDLD on the specified ports.

Default: UDLD packets are untagged; tagged-only ports transmit and receive untagged UDLD control packets

Enabling UDLD (CLI)

UDLD is enabled on a per-port basis.

Example

To enable UDLD on port a1, enter:

```
HP Switch(config)#interface al link-keepalive
```

To enable the feature on a trunk group, enter the appropriate port range. For example:

```
HP Switch(config)#interface al-a4 link-keepalive
```

NOTE: When at least one port is UDLD-enabled, the switch will forward out UDLD packets that arrive on non-UDLD-configured ports out of all other non-UDLDconfigured ports in the same vlan. That is, UDLD control packets will “pass through” a port that is not configured for UDLD. However, UDLD packets will be dropped on any blocked ports that are not configured for UDLD.

Changing the keepalive interval (CLI)

By default, ports enabled for UDLD send a link health-check packet once every 5 seconds. You can change the interval to a value from 10 to 100 deciseconds, where 10 is 1 second, 11 is 1.1 seconds, and so on.

Example

To change the packet interval to seven seconds, enter the following command at the global configuration level:

```
HP Switch(config)# link-keepalive interval 70
```

Changing the keepalive retries (CLI)

By default, a port waits 5 seconds to receive a health-check reply packet from the port at the other end of the link. If the port does not receive a reply, the port tries four more times by sending up to four more health-check packets. If the port still does not receive a reply after the maximum number of retries, the port goes down.

You can change the maximum number of keepalive attempts to a value from 3 to 10.

Example

To change the maximum number of attempts to four, enter the following command at the global configuration level:

```
HP Switch(config)# link-keepalive retries 4
```

Configuring UDLD for tagged ports

The default implementation of UDLD sends the UDLD control packets untagged, even across tagged ports. If an untagged UDLD packet is received by a non-HP switch, that switch may reject the packet. To avoid such an occurrence, you can configure ports to send out UDLD control packets that are tagged with a specified VLAN.

To enable ports to receive and send UDLD control packets tagged with a specific VLAN ID, enter a command such as the following at the interface configuration level:

```
      HP Switch(config)#interface llink-keepalive vlan 22
```

NOTE:

- You must configure the same VLANs that will be used for UDLD on all devices across the network; otherwise, the UDLD link cannot be maintained.
- If a VLAN ID is not specified, UDLD control packets are sent out of the port as untagged packets.
- To re-assign a VLAN ID, re-enter the command with the new VLAN ID number. The new command overwrites the previous command setting.
- When configuring UDLD for tagged ports, you may receive a warning message if there are any inconsistencies with the VLAN configuration of the port (see Table 6 (page 72) for potential problems).

Viewing UDLD information (CLI)

Syntax:

`show link-keepalive`

Displays all the ports that are enabled for `link-keepalive`.

Syntax:

`show link-keepalive statistics`

Displays detailed statistics for the UDLD-enabled ports on the switch.

Syntax:

`clear link-keepalive statistics`

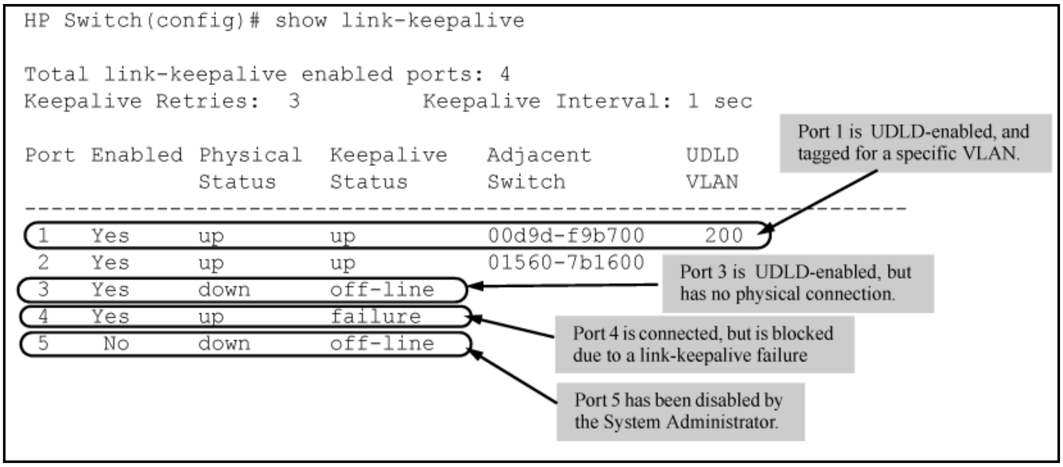
Clears UDLD statistics. This command clears the packets sent, packets received, and transitions counters in the `show link-keepalive statistics` display.

Viewing summary information on all UDLD-enabled ports (CLI)

Enter the `show link-keepalive` command.

Example

Figure 24 Example of `show link-keepalive` command



```
HP Switch(config)# show link-keepalive

Total link-keepalive enabled ports: 4
Keepalive Retries:  3         Keepalive Interval: 1 sec

Port Enabled Physical  Keepalive   Adjacent       UDLD
             Status    Status      Switch         VLAN
-------------------------------------------------------------------
 1   Yes     up        up          00d9d-f9b700    200
 2   Yes     up        up          01560-7b1600
 3   Yes     down      off-line
 4   Yes     up        failure
 5    No     down      off-line
```

Port 1 is UDLD-enabled, and tagged for a specific VLAN.

Port 3 is UDLD-enabled, but has no physical connection.

Port 4 is connected, but is blocked due to a link-keepalive failure

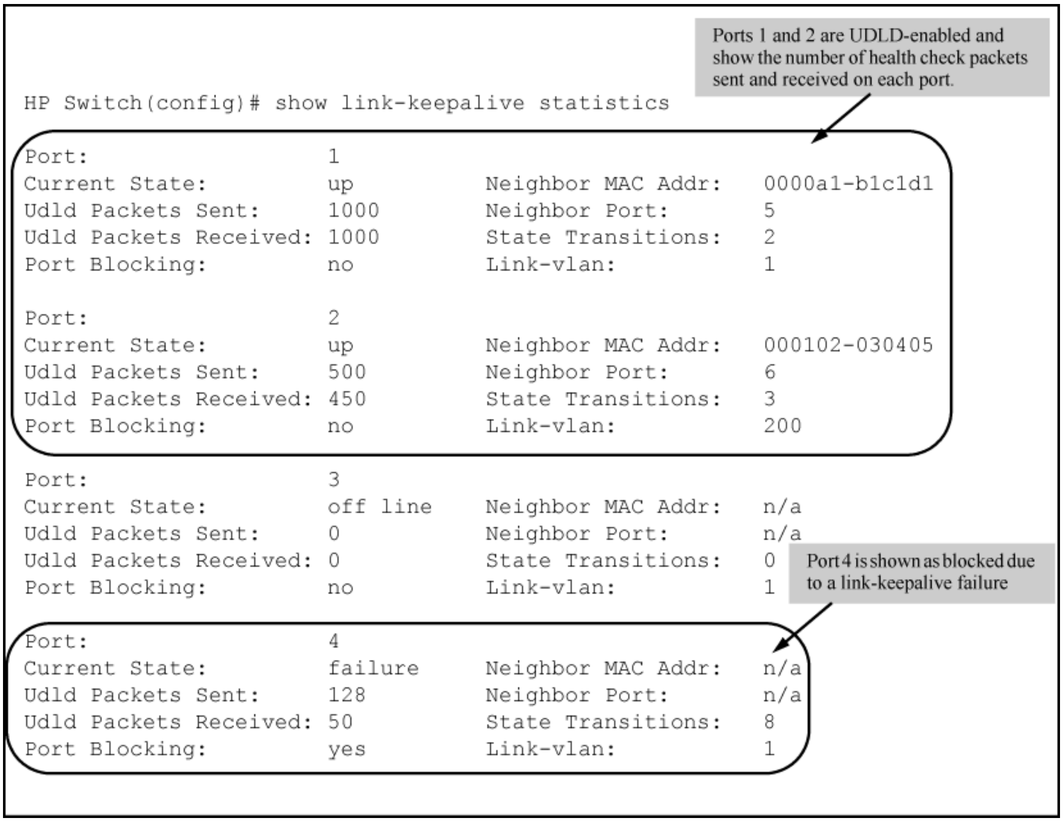
Port 5 has been disabled by the System Administrator.

Viewing detailed UDLD information for specific ports (CLI)

Enter the `show link-keepalive statistics` command.

Example

Figure 25 Example of `show link-keepalive statistics` command



Ports 1 and 2 are UDLD-enabled and show the number of health check packets sent and received on each port.

```
HP Switch(config)# show link-keepalive statistics

Port:                   1
Current State:          up          Neighbor MAC Addr:    0000a1-b1c1d1
Udld Packets Sent:      1000        Neighbor Port:        5
Udld Packets Received:  1000        State Transitions:    2
Port Blocking:          no          Link-vlan:            1

Port:                   2
Current State:          up          Neighbor MAC Addr:    000102-030405
Udld Packets Sent:      500         Neighbor Port:        6
Udld Packets Received:  450         State Transitions:    3
Port Blocking:          no          Link-vlan:            200

Port:                   3
Current State:          off line    Neighbor MAC Addr:    n/a
Udld Packets Sent:      0           Neighbor Port:        n/a
Udld Packets Received:  0           State Transitions:    0
Port Blocking:          no          Link-vlan:            1

Port:                   4
Current State:          failure     Neighbor MAC Addr:    n/a
Udld Packets Sent:      128         Neighbor Port:        n/a
Udld Packets Received:  50          State Transitions:    8
Port Blocking:          yes         Link-vlan:            1
```

Port 4 is shown as blocked due to a link-keepalive failure

Clearing UDLD statistics (CLI)

Enter the following command:

```
HP Switch# clear link-keepalive statistics
```

This command clears the packets sent, packets received, and transitions counters in the `show link keepalive statistics` display (see Figure 25 (page 71) for an example).

Configuring UFD

Syntax:

[no] `uplink-failure-detection`

Globally enables UFD.

The no form of the command globally disables UFD.

Syntax:

[no] `uplink-failure-detection track` *`track-id`* `links-to-monitor [[`*`lacp-key`*`] | [`*`port-list`*`]]`
`links-to-disable [[`*`lacp-key`*`] | [`*`port-list`*`]]`

Configures ports as LtM ports and LtD ports for the specified track. Trunk interfaces are also configurable. The no form of the command removes any track data associated with the specified track.

`track` *`track-id`*	Range is 0–63.
`links-to-monitor [`*`lacp-key`*`|`*`port-list`*`]`	Specifies the lacp key or port list to monitor.
`links-to-disable [`*`lacp-key`*`|`*`port-list`*`]`	Specifies the lacp key or port list to disable.

About viewing port status and configuring port parameters

Connecting transceivers to fixed-configuration devices

If the switch either fails to show a link between an installed transceiver and another device or demonstrates errors or other unexpected behavior on the link, check the port configuration on both devices for a speed and/or duplex (mode) mismatch.

- To check the mode setting for a port on the switch, use either the Port Status screen in the menu interface or `show interfaces brief` in the CLI (see "Viewing port status and configuration (CLI)" (page 52)).
- To display information about the transceivers installed on a switch, enter the `show tech receivers` command in the CLI (Figure 17 (page 57)).

Table 6 Status and parameters for each port type

Status or parameter	Description
Enabled	`Yes` (default): The port is ready for a network connection. `No`: The port will not operate, even if properly connected in a network. Use this setting, for example, if the port needs to be shut down for diagnostic purposes or while you are making topology changes.
Status (read-only)	`Up`: The port senses a link beat. `Down`: The port is not enabled, has no cables connected, or is experiencing a network error. For troubleshooting information, see the *Installation and Getting Started Guide* you received with the switch. See also to Appendix C, "Troubleshooting" (in this manual).
Mode	The port's speed and duplex (data transfer operation) setting.

Table 6 Status and parameters for each port type *(continued)*

Status or parameter	Description
	`10/100/1000Base-T Ports:` • `Auto-MDIX` (default): Senses speed and negotiates with the port at the other end of the link for port operation (MDI-X or MDI). To see what the switch negotiates for the auto setting, use theCLI `show interfaces brief` command or the `3. Port Status` option under `1. Status and Counters` in the menu interface. • `MDI`: Sets the port to connect with a PC using a crossover cable (manual mode—applies only to copper port switches using twisted-pair copper Ethernet cables) • `MDIX`: Sets the port to connect with a PC using a straight-through cable (manual mode—applies only to copper port switches using twisted-pair copper Ethernet cables) • `Auto-10`: Allows the port to negotiate between half-duplex (HDx) and full-duplex (FDx) while keeping speed at 10 Mbps. Also negotiates flow control (enabled or disabled). HP recommends auto-10 for links between 10/100 auto-sensing ports connected with Cat 3 cabling. (Cat 5 cabling is required for 100 Mbps links.). • `10HDx`:10 Mbps, half-duplex • `10FDx`: 10 Mbps, full-duplex • `Auto-100`: Uses 100 Mbps and negotiates with the port at the other end of the link for other port operation features. • `Auto-10-100`: Allows the port to establish a link with the port at the other end at either 10 Mbps or 100 Mbps, using the highest mutual speed and duplex mode available. Only these speeds are allowed with this setting. • `Auto-1000`: Uses 1000 Mbps and negotiates with the port at the other end of the link for other port operation features. • `100Hdx`: Uses 100 Mbps, half-duplex. • `100Fdx`: Uses 100 Mbps, full-duplex **Gigabit Fiber-Optic Ports (Gigabit-SX, Gigabit-LX, and Gigabit-LH):** • `1000FDx`: 1000 Mbps (1 Gbps), full-duplex only • `Auto` (default): The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port. **Gigabit Copper Ports:** • `1000FDx`: 1000 Mbps (1 Gbps), full-duplex only • `Auto` (default): The port operates at 1000FDx and auto-negotiates flow control with the device connected to the port. **10-Gigabit CX4 Copper Ports:** • Auto: The port operates at 10 gigabits FDx and negotiates flow control. Lower speed settings or half-duplex are not allowed. **10-Gigabit SC Fiber-Optic Ports (10-GbE SR, 10-GbE LR, 10-GbE ER):** • Auto: The port operates at 10 gigabits FDx and negotiates flow control. Lower speed settings or half-duplex are not allowed. **NOTE:** Conditioning patch cord cables are not supported on 10-GbE.
Auto-MDIX	The switch supports Auto-MDIX on 10Mb, 100Mb, and 1 Gb T/TX (copper) ports. (Fiber ports and 10-gigabit ports do not use this feature.) • `Automdix`: Configures the port for automatic detection of the cable type (straight-through or crossover). • `MDI`: Configures the port to connect to a switch, hub, or other MDI-X device with a straight-through cable. • `MDIX`: Configures the port to connect to a PC or other MDI device with a straight-through cable.

Table 6 Status and parameters for each port type *(continued)*

Status or parameter	Description
Flow control	- `Disabled` (default): The port does not generate flow control packets, and drops any flow control packets it receives. - `Enabled`: The port uses 802.3x link layer flow control, generates flow-control packets, and processes received flow-control packets. With the port mode set to `Auto` (the default) and flow control enabled, the switch negotiates flow control on the indicated port. If the port mode is not set to `Auto`, or if flow control is disabled on the port, flow control is not used. Note that flow control must be enabled on both ends of a link.
Broadcast limit	Specifies the percentage of the theoretical maximum network bandwidth that can be used for broadcast traffic. Any broadcast traffic exceeding that limit will be dropped. Zero (0) means the feature is disabled. The broadcast-limit command operates at the port context level to set the broadcast limit for a port on the switch. **NOTE:** This feature is not appropriate for networks that require high levels of IPX or RIP broadcast traffic.

Error messages associated with the show interfaces command

Error	Error message
Requesting too many fields (total characters exceeds 80)	Total length of selected data exceeds one line
Field name is misspelled	Invalid input: *`input`*
Mistake in specifying the port list	Module not present for port or invalid port: *`input`*
The port list is not specified	Incomplete input: custom

Note on using pattern matching with the `show interfaces` custom command

If you have included a pattern matching command to search for a field in the output of the `show int custom` command, and the `show int custom` command produces an error, the error message may not be visible and the output is empty. For example, if you enter a command that produces an error (such as vlan is misspelled) with the pattern matching `include` option, the output may be empty:

```
[ HP Switch(config)# show int custom 1-3 name vlun  |   include
vlan1 ]
```

It is advisable to try the `show int custom` command first to ensure there is output, and then enter the command again with the pattern matching option.

Note that in the above command, you can substitute `int` for `interface`; that is: show `int custom`.

About configuring auto-MDIX

Copper ports on the switch can automatically detect the type of cable configuration (MDI or MDI-X) on a connected device and adjust to operate appropriately.

This means you can use a "straight-through" twisted-pair cable or a "crossover" twisted-pair cable for any of the connections—the port makes the necessary adjustments to accommodate either one for correct operation. The following port types on your switch support the IEEE 802.3ab standard, which includes the "Auto MDI/MDI-X" feature:

- 10/100-TX xl module ports
- 100/1000-T xl module ports
- 10/100/1000-T xl module ports

Using the above ports:

- If you connect a copper port using a straight-through cable on a switch to a port on another switch or hub that uses MDI-X ports, the switch port automatically operates as an MDI port.
- If you connect a copper port using a straight-through cable on a switch to a port on an end node—such as a server or PC—that uses MDI ports, the switch port automatically operates as an MDI-X port.

HP Switch auto-MDIX supports operation in forced speed and duplex modes.

For more information on this subject, see the *IEEE 802.3ab Standard Reference*. For more information on MDI-X, see the *Installation and Getting Started Guide* for your switch.

Manual override

If you require control over the MDI/MDI-X feature, you can set the switch to either of these non-default modes:

- Manual MDI
- Manual MDI-X

Table 7 (page 75) shows the cabling requirements for the MDI/MDI-X settings.

Table 7 Cable types for auto and manual MDI/MDI-X settings

Setting	MDI/MDI-X device type	
	PC or other MDI device type	Switch, hub, or other MDI-X device
Manual MDI	Crossover cable	Straight-through cable
Manual MDI-X	Straight-through cable	Crossover cable
Auto-MDI-X (the default)	Either crossover or straight-through cable	

The AutoMDIX features apply only to copper port switches using twisted-pair copper Ethernet cables.

About using friendly (optional) port names

This feature enables you to assign alphanumeric port names of your choosing to augment automatically assigned numeric port names. This means you can configure meaningful port names to make it easier to identify the source of information listed by some `show` commands. (Note that this feature *augments* port numbering, but *does not replace* it.)

Configuring and operating rules for friendly port names

- At either the global or context configuration level, you can assign a unique name to a port. You can also assign the same name to multiple ports.
- The friendly port names you configure appear in the output of the `show name` *`port-list`*, `show config`, and `show interface` *`port-number`* commands. They do not appear in the output of other `show` commands or in Menu interface screens. (See "Displaying friendly port names with other port data (CLI)" (page 65).)
- Friendly port names are not a substitute for port numbers in CLI commands or Menu displays.

- Trunking ports together does not affect friendly naming for the individual ports. (If you want the same name for all ports in a trunk, you must individually assign the name to each port.)
- A friendly port name can have up to 64 contiguous alphanumeric characters.
- Blank spaces within friendly port names are not allowed, and if used, cause an **invalid input** error. (The switch interprets a blank space as a name terminator.)
- In a port listing, **not assigned** indicates that the port does not have a name assignment other than its fixed port number.
- To retain friendly port names across reboots, you must save the current running-configuration to the startup-config file after entering the friendly port names. (In the CLI, use the `write memory` command.)

About configuring transceivers and modules that have not been inserted

Transceivers

Previously, a port had to be valid and verified for the switch to allow it to be configured. Transceivers are removable ports and considered invalid when not present in the switch, so they cannot be configured unless they are already in the switch. For HP switches, the verification for allowable port configurations performed by the CLI is removed and configuration of transceivers is allowed even if they are not yet inserted in the switch.

Modules

You can create or edit configuration files (as text files) that can be uploaded to the switch without the modules having been installed yet. Additionally, you can pre-configure the modules with the CLI `module` command.

The same `module` command used in an uploaded configuration file is used to define a module that is being pre-configured. The validation performed when issued through the CLI is still performed just as if the command was executed on the switch, in other words, as if the module were actually present in the switch.

NOTE: You cannot use this method to change the configuration of a module that has already been configured. The slot must be empty and the configuration file must not have a configuration associated with it.

About clearing the module configuration

Because of the hot-swap capabilities of the modules, when a module is removed from the chassis, the module configuration remains in the configuration file. `[no] module slot` allows you to remove the module configuration information from the configuration file.

NOTE: This does not change how hot-swap works.

Restrictions

The following restrictions apply:

- The slot being cleared must be empty
- There was no module present in the slot since the last boot
- If there was a module present after the switch was booted, the switch will have to be rebooted before any module (new or same) can be used in the slot.
- This does not clear the configuration of a module still in use by the switch.

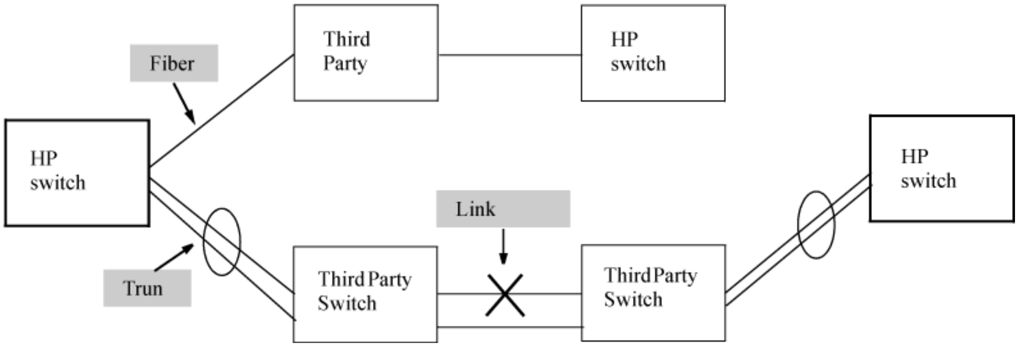
Uni-directional link detection (UDLD)

Uni-directional link detection (UDLD) monitors a link between two HP switches and blocks the ports on both ends of the link if the link fails at any point between the two devices. This feature is particularly useful for detecting failures in fiber links and trunks. Figure 26 (page 77) shows an example.

Figure 26 UDLD example

Scenario 1 (No UDLD): Without UDLD, the switch ports remain enabled despite the link failure. Traffic continues to be load-balanced to the ports connected to the failed link.

Scenario 2 (UDLD-enabled): When UDLD is enabled, the feature blocks the ports connected to the failed link.



In this example, each HP switch load balances traffic across two ports in a trunk group. Without the UDLD feature, a link failure on a link that is not directly attached to one of the HP switches remains undetected. As a result, each switch continue to send traffic on the ports connected to the failed link. When UDLD is enabled on the trunk ports on each HP switch, the switches detect the failed link, block the ports connected to the failed link, and use the remaining ports in the trunk group to forward the traffic.

Similarly, UDLD is effective for monitoring fiber optic links that use two uni-direction fibers to transmit and receive packets. Without UDLD, if a fiber breaks in one direction, a fiber port may assume the link is still good (because the other direction is operating normally) and continue to send traffic on the connected ports. UDLD-enabled ports; however, will prevent traffic from being sent across a bad link by blocking the ports in the event that either the individual transmitter or receiver for that connection fails.

Ports enabled for UDLD exchange health-check packets once every five seconds (the link-keepalive interval). If a port does not receive a health-check packet from the port at the other end of the link within the keepalive interval, the port waits for four more intervals. If the port still does not receive a health-check packet after waiting for five intervals, the port concludes that the link has failed and blocks the UDLD-enabled port.

When a port is blocked by UDLD, the event is recorded in the switch log or via an SNMP trap (if configured); and other port blocking protocols, like spanning tree or meshing, will not use the bad link to load balance packets. The port will remain blocked until the link is unplugged, disabled, or fixed. The port can also be unblocked by disabling UDLD on the port.

About Configuring UDLD

When configuring UDLD, keep the following considerations in mind:

- UDLD is configured on a per-port basis and must be enabled at both ends of the link. See the note below for a list of HP switches that support UDLD.
- To configure UDLD on a trunk group, you must configure the feature on each port of the group individually. Configuring UDLD on a trunk group's primary port enables the feature on that port only.
- Dynamic trunking is not supported. If you want to configure a trunk group that contains ports on which UDLD is enabled, you must remove the UDLD configuration from the ports. After you create the trunk group, you can re-add the UDLD configuration.

NOTE: UDLD interoperates with the following HP switches: 2600, 2800, 3400, 3500, 4200, 5300, 5400, 6200, 6400, 6600, 8212, and 9300. Consult the release notes and current manuals for required software versions.

When at least one port is UDLD-enabled, the switch will forward out UDLD packets that arrive on non-UDLD-configured ports out of all other non-UDLD-configured ports in the same vlan. That is, UDLD control packets will "pass through" a port that is not configured for UDLD. However, UDLD packets will be dropped on any blocked ports that are not configured for UDLD.

About Uplink failure detection

Uplink Failure Detection (UFD) is a network path redundancy feature that works in conjunction with NIC teaming functionality. UFD continuously monitors the link state of the ports configured as links-to-monitor (LtM), and when these ports lose link with their partners, UFD will disable the set of ports configured as links-to-disable (LtD). When an uplink port goes down, UFD enables the switch to auto-disable the specific downlinks connected to the NICs. This allows the NIC teaming software to detect link failure on the primary NIC port and fail over to the secondary NIC in the team.

NIC teams must be configured for switch redundancy when used with UFD, that is, the team spans ports on both Switch A and Switch B. The switch automatically enables the downlink ports when the uplink returns to service. For an example of teamed NICs in conjunction with UFD, see Figure 27 (page 79)). For an example of teamed NICs with a failed uplink, see Figure 28 (page 79).

NOTE: For UFD functionality to work as expected, the NIC teaming must be in Network Fault Tolerance (NFT) mode.

Figure 27 Example of teamed NICs in conjunction with UFD

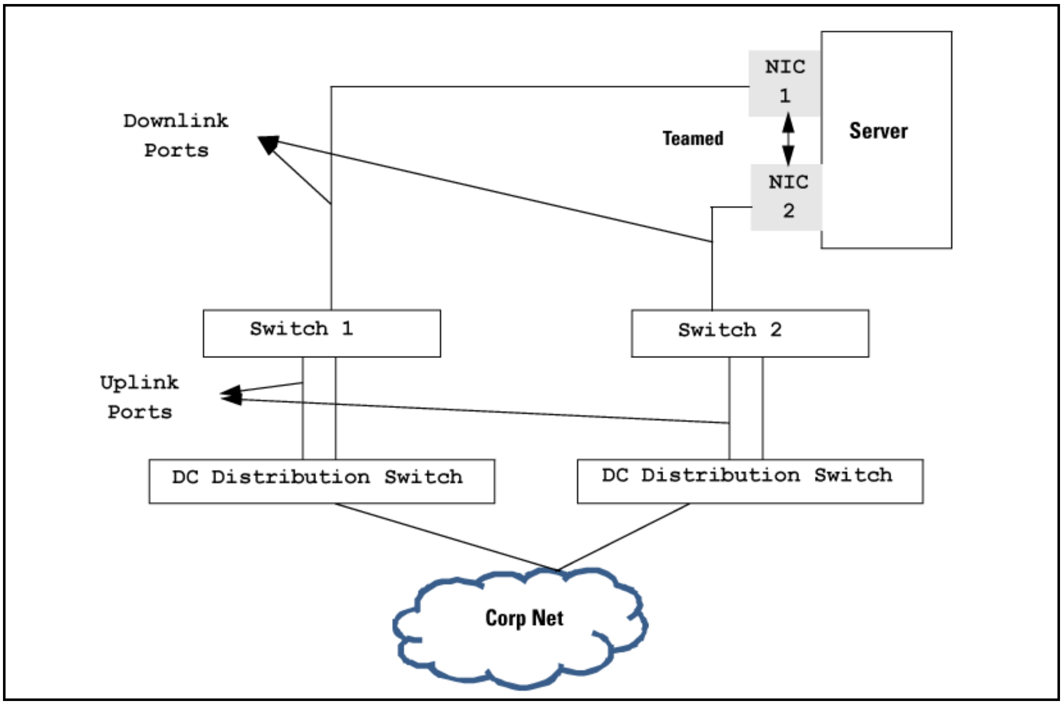
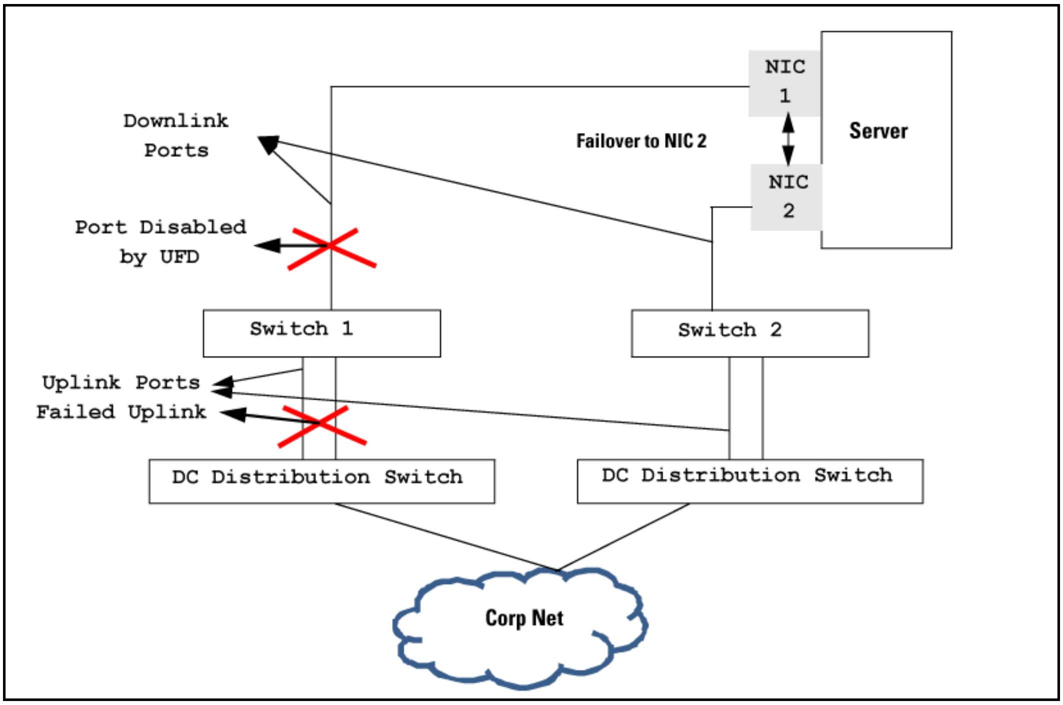


Figure 28 Example of teamed NICs with a failed uplink



UFD operating notes

- A port cannot be added to a trunk group if it already belongs to an LtM or LtD.
- Ports that are already members of a trunk group cannot be assigned to an LtM or LtD.
- Trunks that are configured as LtM or LtD cannot be deleted.

Example 30 Configuring ports as LtM and LtD for track 3

```
HP Switch(config)# uplink-failure-detection track 3 links-to-monitor 5,6,7
links-to-disable 8,9,10
```

Example 31 Removing a LtM port and an LtD port for track 3

```
HP Switch(config)# no uplink-failure-detection track 3 links-to-monitor 5
links-to-disable 8
```

Viewing UFD configuration

Enter the `show uplink-failure-detection` command to display information about the UFD configuration.

Example 32 Displaying informationn for UFD configuration

```
HP Switch(config)# show uplink-failure-detection
UFD State: Enabled

Failure Detection Pairs:

  TRACK ID | Monitored Links Links to Disable LtM State LtD State
  -------- + --------------- ---------------- --------- ---------------
  3          5,6             D3               Up        Up
  4          13              D4,D5            Down      Auto-Disabled
```

4 Power Over Ethernet (PoE/PoE+) Operation

Command Summary

Table 8 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
`[ no ]interface` *`port-list`* `power-over-ethernet`	Re-enables PoE operation on *`port-list`* and restores the priority setting in effect when PoE was disabled on *`port-list`*	-	(page 83)	-
`[ no ]power-over-ethernet pre-std-detect`	Detects and powers pre-802.3af standard devices	-	(page 83)	-
`interface` *`port-list`* `power-over-ethernet[ critical | high | low ]`	Reconfigures the PoE priority level on *`port-list`*	Low	(page 83)	-
`[ no ]int` *`port-list`* `poe-allocate-by[ usage | class | value ]`	Allows you to manually allocate the amount of PoE power for a port by either its class or a defined value	Usage	(page 84)	-
`[no] power-over-ethernet redundancy[ n+1 | full ]`	Allows you to set the amount of power held in reserve for redundancy	No	(page 85)	-
`power-over-ethernet[ slot` *`slot-id-range`* `]`*`threshold 1 - 99`*	Specifies the PoE usage level (as a percentage of the PoE power available on a module) at which the switch generates a power usage notice	-	(page 86)	-

Table 8 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`int` *`port-list`* `poe-lldp-detect [ enabled | disabled ]`	Enables or disables ports for allocating PoE power based on the link-partner's capabilities via LLDP.	Disabled	(page 86)	-
`int` *`port-list`* `PoE-lldp-detect [ enabled | disabled ]`	Allows the data link layer to be used for power negotiation between a PD on a PoE port and LLDP.	Disabled	(page 86)	-
`lldp config` *`port-list`* `dot3TlvEnable poeplus_config`	Enables advertisement of data link layer power using PoE+ TLVs	Enabled	(page 87)	-
`show lldp config` *`port-list`*	Displays the LLDP port configuration information, including the TLVs advertised.	-	(page 88)	-
`show power-over-ethernet [ brief | [ethernet]`*`port-list`* `| [ slot` *`slot-id-range`* `| all ] ]`	Displays the switch's global PoE power status	-	(page 89)	-
`show power-over-ethernet brief`	Displays the port power status	-	(page 90)	-
`show power-over-ethernet` *`port-list`*	Displays PoE status and statistics (since the last reboot) for each port in *`port-list`*	-	(page 92)	-

Introduction to PoE

PoE technology allows IP telephones, wireless LAN access points, and other appliances to receive power and transfer data over existing ethernet LAN cabling. For more information about PoE technology, see the *PoE Planning and Implementation Guide*, which is available on the HP Networking website at

www.hp.com/networking/support.

PoE terminology

Power-over-ethernet (PoE) and Power-over-ethernet plus (PoE+ or POEP) operate similarly in most cases. The CLI commands are the same for a PoE module or a PoE+ zl module. Any differences between PoE and PoE+ operation are noted; otherwise, the term "PoE" is used to designate both PoE and PoE+ functionality.

Disabling or re-enabling PoE port operation

Syntax:

```
[no] interface port-list power-over-ethernet
```

Re-enables PoE operation on *port-list* and restores the priority setting in effect when PoE was disabled on *port-list*.

The no form of the command disables PoE operation on *port-list*.

Default: All PoE ports are initially enabled for PoE operation at Low priority. If you configure a higher priority, this priority is retained until you change it.

NOTE: For PoE, disabling all ports allows the 22 watts of minimum PoE power or the 38 watts for PoE+ power allocated for the module to be recovered and used elsewhere. You must disable ALL ports for this to occur.

Enabling support for pre-standard devices

Syntax:

The HP switches covered in this guide also support some pre-802.3af devices. For a list of the supported devices, see the FAQ for your switch model.

```
[no] power-over-ethernet pre-std-detect
```

Detects and powers pre-802.3af standard devices.

NOTE: The default setting for the `pre-std-detect` PoE parameter has changed. In earlier software, the default setting is "on." In K.15.02 and later software, the default setting is "off."

Configuring the PoE port priority

Syntax:

```
interface port-list power-over-ethernet [ critical | high | low ]
```

Reconfigures the PoE priority level on *port-list*. For a given level, ports

`Critical`	Specifies the highest-priority PoE support for *port-list*. The active PoE ports at this level are provisioned before the PoE ports at any other level are provisioned.
`High`	Specifies the second priority PoE support for *port-list*. The active PoE ports at this level are provisioned before the `Low` priority PoE ports are provisioned.
`Low`	(Default) Specifies the third priority PoE support for *port-list*. The active PoE ports at this level are provisioned only if there is power available after provisioning any active PoE ports at the higher priority levels.

For more information configuring PoE port priority and on assigning PoE priority on more than one module, see "About assigning PoE priority with two or more modules" (page 97).

Controlling PoE allocation

Syntax:

`[no] int port-list poe-allocate-by[ usage | class | value ]`

Allows you to manually allocate the amount of PoE power for a port by either its class or a defined value.

The default option for PoE allocation is usage, which is what a PD attached to the port is allocated. You can override this value by specifying the amount of power allocated to a port by using the class or value options.

`usage` (Default) The automatic allocation by a PD.

`class` Uses the power ramp-up signature of the PD to identify which power class the device will be in. Classes and their ranges are shown in Table 9 (page 84).

`value` A user-defined level of PoE power allocated for that port.

NOTE: The allowable PD requirements are lower than those specified for PSEs to allow for power losses along the Cat-5 cable.

Table 9 Power classes and their values

Power class	Value
0	Depends on cable type and PoE architecture. Maximum power level output of 15.4 watts at the PSE. This is the default class; if there is not enough information about the load for a specific classification, the PSE classifies the load as class 0 (zero).
1	Requires at least 4 watts at the PSE.
2	Requires at least 7 watts at the PSE.
3	15.4 watts
4	For PoE+ Maximum power level output of 30 watts at the PSE.

Example

To allocate by class for ports 6 to 8:

```
HP Switch(config)# int 6-8 PoE-allocate-by class
```

Manually configuring PoE power levels

You can specify a power level (in watts) allocated for a port by using the `value` option. This is the maximum amount of power that will be delivered.

1. To configure a port by value, first set the PoE allocation by entering the `poe-allocate-by value` command:

   ```
   HP Switch(config) # int A6 poe-allocate-by value
   ```

   or in interface context:

   ```
   HP Switch(eth-A6) # poe-allocate-by value
   ```

2. Then select a value:

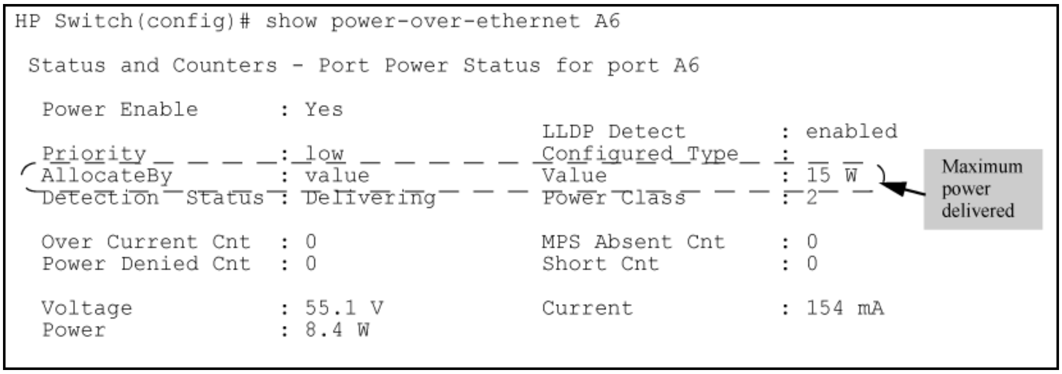
   ```
   HP Switch(config) # int A6 poe-value 15
   ```

   or in interface context:

   ```
   HP Switch(eth-A6) # poe-value 15
   ```

3. To view the settings, enter the `show power-over-ethernet` command, shown in Figure Figure 29 (page 85).

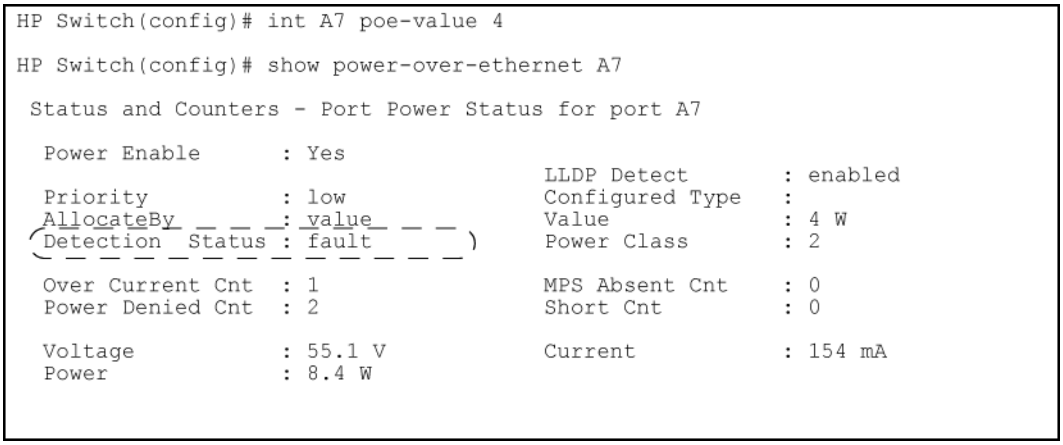
Figure 29 Example displaying PoE allocation by value and the maximum power delivered



```
HP Switch(config)# show power-over-ethernet A6

 Status and Counters - Port Power Status for port A6

  Power Enable       : Yes
                                      LLDP Detect        : enabled
  Priority           : low            Configured Type    :
  AllocateBy         : value          Value              : 15 W
  Detection  Status  : Delivering     Power Class        : 2

  Over Current Cnt   : 0              MPS Absent Cnt     : 0
  Power Denied Cnt   : 0              Short Cnt          : 0

  Voltage            : 55.1 V         Current            : 154 mA
  Power              : 8.4 W
```

If you set the PoE maximum value to less than what the PD requires, a **fault** occurs, as shown in Figure Figure 30 (page 85).

Figure 30 Example showing PoE power value set too low for the PD



```
HP Switch(config)# int A7 poe-value 4

HP Switch(config)# show power-over-ethernet A7

 Status and Counters - Port Power Status for port A7

  Power Enable       : Yes
                                      LLDP Detect        : enabled
  Priority           : low            Configured Type    :
  AllocateBy         : value          Value              : 4 W
  Detection  Status  : fault          Power Class        : 2

  Over Current Cnt   : 1              MPS Absent Cnt     : 0
  Power Denied Cnt   : 2              Short Cnt          : 0

  Voltage            : 55.1 V         Current            : 154 mA
  Power              : 8.4 W
```

Configuring PoE redundancy (chassis switches only)

PoE redundancy occurs automatically when enabled. The switch keeps track of power use and does not supply PoE power to additional PoE devices trying to connect if that results in the switch not having enough power in reserve for redundancy.

Syntax:

`[no] power-over-ethernet redundancy [ n+1 | full ]`

Allows you to set the amount of power held in reserve for redundancy.

`no`	Means that all available power can be allocated to PDs. Default: No PoE redundancy enforced.
`n+1`	One of the power supplies is held in reserve for redundancy. If a single power supply fails, no powered devices are shut down. If power supplies with different ratings are used, the highest-rated power supply is held in reserve to ensure full redundancy.
`full`	Half of the available power supply is held in reserve for redundancy. If power supplies with different ratings are used, the highest-rated power supply is held in reserve to ensure full redundancy.

For more information about PoE redundancy and power supplies, see the *PoE Planning and Implementation Guide*, available on the HP website at

www.hp.com/networking/support.

Changing the threshold for generating a power notice

Syntax:

`power-over-ethernet [ slot *slot-id-range* ] *threshold 1 - 99*`

Specifies the PoE usage level (as a percentage of the PoE power available on a module) at which the switch generates a power usage notice. This notice appears as an SNMP trap and a corresponding Event Log message and occurs when a PoE module's power consumption crosses the configured threshold value. That is, the switch generates a notice whenever the power consumption on a module either exceeds or drops below the specified percentage of the total PoE power available on the module.

This command configures the notification threshold for PoE power usage on either a global or per-module (slot) basis.

Without the `[slot PoE *slot-id-range*]` option, the switch applies one power threshold setting on all PoE modules installed in the switch.

For more information on configuring thresholds, see “About configuring thresholds for generating a power notice” (page 99).

Enabling or disabling ports for allocating power using LLDP

Syntax:

`int *port-list* poe-lldp-detect [ enabled | disabled ]`

Enables or disables ports for allocating PoE power based on the link-partner's capabilities via LLDP.

Default: Disabled

Example

You can enter this command to enable LLDP detection:

```
HP Switch(config) # int A7 poe-lldp-detect enabled
```

or in interface context:

```
HP Switch(eth-A7) # poe-lldp-detect enabled
```

For more information on PoE/PoE+ and LLDP, see “About PoE/PoE+ allocation using LLDP information” (page 100).

Enabling PoE detection via LLDP TLV advertisement

Use this command and insert the desired port or ports:

```
        HP Switch(config) # lldp config port-number
        medTlvenable poe
```

For more information on LLDP, see “About PoE/PoE+ allocation using LLDP information” (page 100).

Negotiating power using the DLL

When a PD requests power on a PoE port, LLDP interacts with PoE to see if there is enough power to fulfill the request. Power is set at the level requested. If the PD goes into power-saving mode, the power supplied is reduced; if the need for power increases, the amount supplied increases. PoE and LLDP interact to meet the current power demands.

Syntax:

`int` *`port-list`*`PoE-lldp-detect [ enabled | disabled ]`

Allows the data link layer to be used for power negotiation between a PD on a PoE port and LLDP.

Default: Disabled

Example

You can enter this command to enable LLDP detection:

```
HP Switch(config) # int 7 PoE-lldp-detect enabled
```

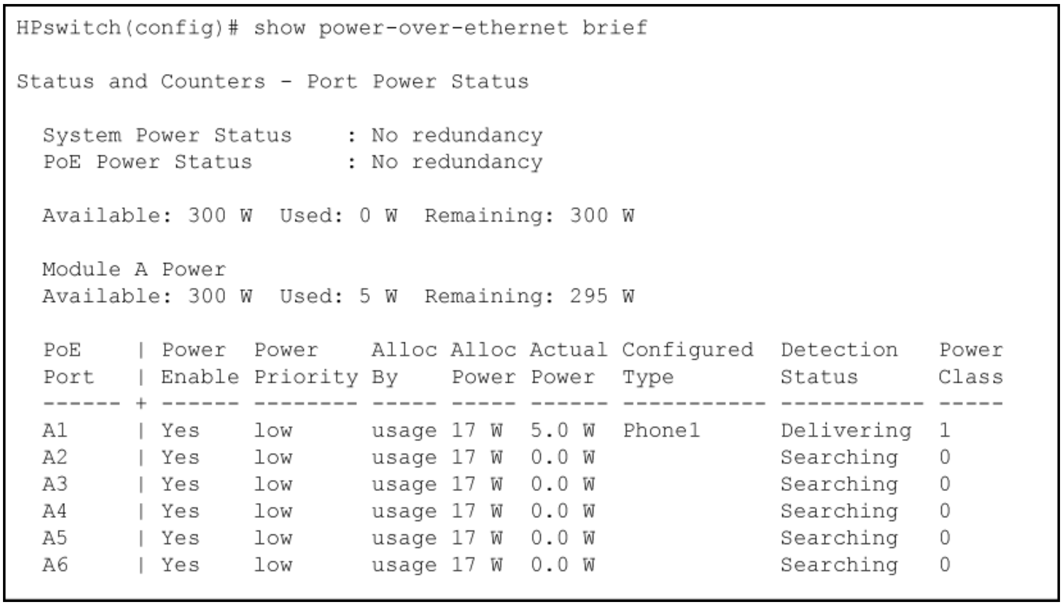
or in interface context:

```
HP Switch(eth-7) # PoE-lldp-detect enabled
```

NOTE: Detecting PoE information via LLDP affects only power delivery; it does not affect normal Ethernet connectivity.

You can view the settings by entering the `show power-over-ethernet brief` command, as shown in Figure Figure 31 (page 87).

Figure 31 Example of port with LLDP configuration information obtained from the device



```
HPswitch(config)# show power-over-ethernet brief

Status and Counters - Port Power Status

  System Power Status     : No redundancy
  PoE Power Status        : No redundancy

  Available: 300 W  Used: 0 W  Remaining: 300 W

  Module A Power
  Available: 300 W  Used: 5 W  Remaining: 295 W

  PoE    | Power  Power    Alloc Alloc Actual Configured  Detection   Power
  Port   | Enable Priority By    Power Power  Type         Status      Class
  ------ + ------ -------- ----- ----- ------ ----------- ----------- -----
  A1     | Yes    low      usage 17 W  5.0 W  Phone1      Delivering  1
  A2     | Yes    low      usage 17 W  0.0 W              Searching   0
  A3     | Yes    low      usage 17 W  0.0 W              Searching   0
  A4     | Yes    low      usage 17 W  0.0 W              Searching   0
  A5     | Yes    low      usage 17 W  0.0 W              Searching   0
  A6     | Yes    low      usage 17 W  0.0 W              Searching   0
```

Initiating advertisement of PoE+ TLVs

Syntax:

`lldp config` *`port-list`* `dot3TlvEnable poeplus_config`

Enables advertisement of data link layer power using PoE+ TLVs.The TLV is processed only after the physical layer and the data link layer are enabled. The TLV informs the PSE about the actual power required by the device.

Default: Enabled

NOTE: If LLDP is disabled at runtime, and a PD is using PoE+ power that has been negotiated through LLDP, there is a temporary power drop; the port begins using PoE+ power through the PLC. This event is recorded in the Event Log. An example message would look like the following:

```
W 08/04/10 13:35:50 02768 ports: Port A1 PoE power dropped.
Exceeded physical classification for a PoE Type1 device (LLDP process
disabled)
```

When LLDP is enabled again, it causes a temporary power drop. This event is also recorded in the Event Log. An example message looks like the following:

```
W 08/04/10 13:36:31 02771 ports: Port A1 PoE power dropped.
Exceeded physical classification due to change in classification type (LLDP process
 enabled)
```

Viewing PoE when using LLDP information

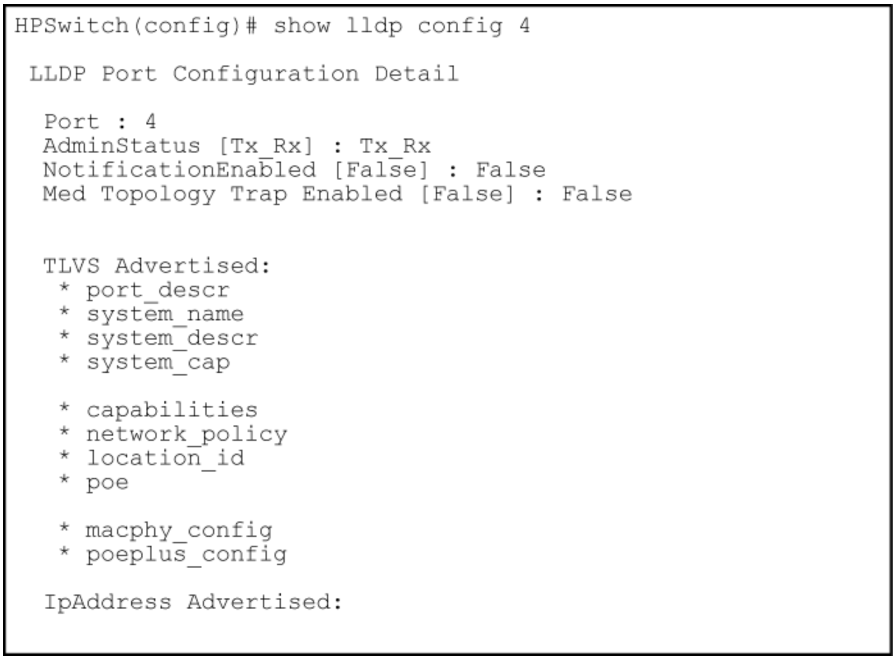
Syntax:

`show lldp config` *`port-list`*

Displays the LLDP port configuration information, including the TLVs advertised.

Examples

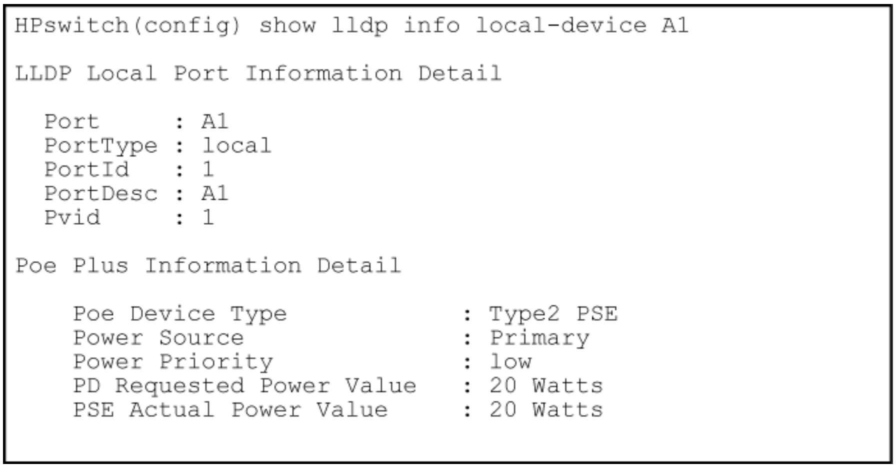
Figure 32 LLDP port configuration information with PoE



```
HPSwitch(config)# show lldp config 4

 LLDP Port Configuration Detail

  Port : 4
  AdminStatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False


  TLVS Advertised:
   * port_descr
   * system_name
   * system_descr
   * system_cap

   * capabilities
   * network_policy
   * location_id
   * poe

   * macphy_config
   * poeplus_config

  IpAddress Advertised:
```

Figure Figure 33 (page 89) shows an example of the local device power information using the `show lldp info local-device` *`port-list`* command.

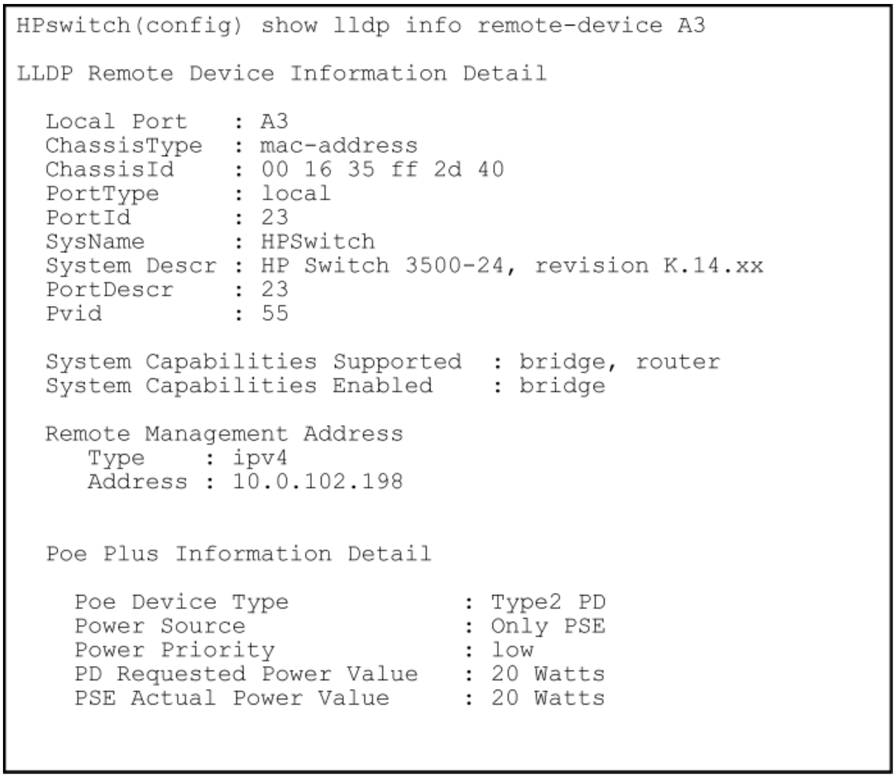
Figure 33 Local power information



```
HPswitch(config) show lldp info local-device A1

LLDP Local Port Information Detail

  Port     : A1
  PortType : local
  PortId   : 1
  PortDesc : A1
  Pvid     : 1

Poe Plus Information Detail

    Poe Device Type              : Type2 PSE
    Power Source                 : Primary
    Power Priority               : low
    PD Requested Power Value     : 20 Watts
    PSE Actual Power Value       : 20 Watts
```

Figure Figure 34 (page 89) shows an example of the remote device power information using the `show lldp info remote-device` *`port-list`* command.

Figure 34 Remote power information



```
HPswitch(config) show lldp info remote-device A3

LLDP Remote Device Information Detail

  Local Port   : A3
  ChassisType  : mac-address
  ChassisId    : 00 16 35 ff 2d 40
  PortType     : local
  PortId       : 23
  SysName      : HPSwitch
  System Descr : HP Switch 3500-24, revision K.14.xx
  PortDescr    : 23
  Pvid         : 55

  System Capabilities Supported  : bridge, router
  System Capabilities Enabled    : bridge

  Remote Management Address
     Type    : ipv4
     Address : 10.0.102.198


  Poe Plus Information Detail

    Poe Device Type              : Type2 PD
    Power Source                 : Only PSE
    Power Priority               : low
    PD Requested Power Value     : 20 Watts
    PSE Actual Power Value       : 20 Watts
```

Viewing the global PoE power status of the switch

Syntax:

`show power-over-ethernet [ brief | [ethernet]`*`port-list`*` | [ slot `*`slot-id-range`*` | all ] ]`

Displays the switch's global PoE power status, including:

- **Total Available Power**

  Lists the maximum PoE wattage available to provision active PoE ports on the switch. This is the amount of usable power for PDs.

- **Total Failover Power**

  Lists the amount of PoE power available in the event of a single power supply failure. This is the amount of power the switch can maintain without dropping any PDs.

- **Total Redundancy Power**

  Indicates the amount of PoE power held in reserve for redundancy in case of a power supply failure.

- **Total Remaining Power**

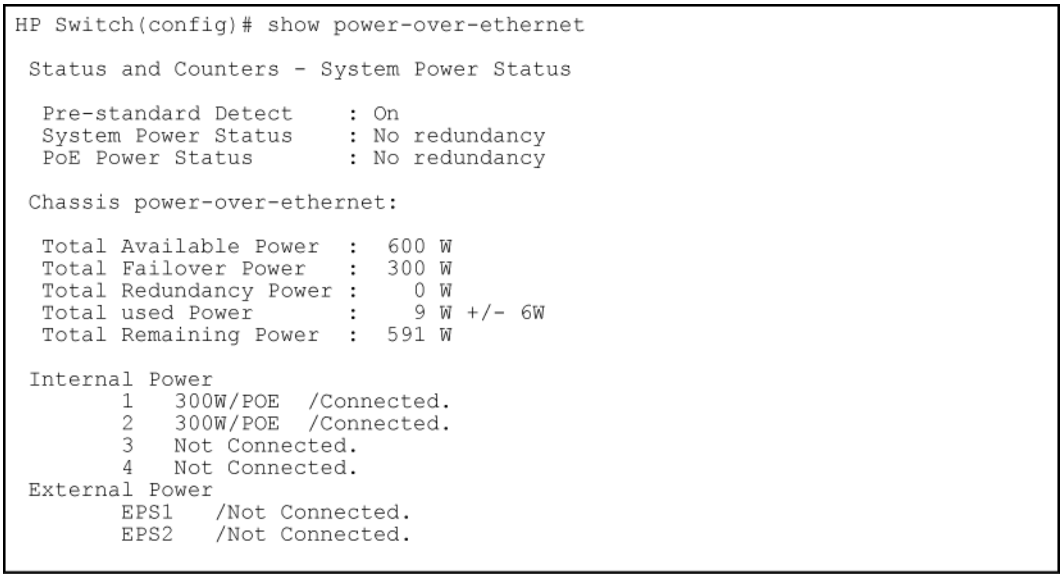
  The amount of PoE power still available.

`brief`	Displays PoE information for each port. See "Viewing PoE status on all ports" (page 90).
`port-list`	Displays PoE information for the ports in port-list. See "Viewing the PoE status on specific ports" (page 92).
`slot-id-range`	Displays PoE information for the selected slots. (See figure Figure 37 (page 92)). Enter the `all` option to display the PoE information for all slots.

Example

`show power-over-ethernet` displays data similar to that shown in Figure Figure 35 (page 90).

Figure 35 `show power-over-ethernet` command output



```
HP Switch(config)# show power-over-ethernet

 Status and Counters - System Power Status

  Pre-standard Detect     : On
  System Power Status     : No redundancy
  PoE Power Status        : No redundancy

 Chassis power-over-ethernet:

  Total Available Power   :  600 W
  Total Failover Power    :  300 W
  Total Redundancy Power  :    0 W
  Total used Power        :    9 W +/- 6W
  Total Remaining Power   :  591 W

 Internal Power
        1   300W/POE  /Connected.
        2   300W/POE  /Connected.
        3   Not Connected.
        4   Not Connected.
 External Power
        EPS1   /Not Connected.
        EPS2   /Not Connected.
```

Viewing PoE status on all ports

Syntax:

`show power-over-ethernet brief`

Displays the port power status, including:

- **PoE Port**

  Lists all PoE-capable ports on the switch.

- **Power Enable**

  Shows **Yes** for ports enabled to support PoE (the default) and **No** for ports on which PoE is disabled.

- **Power Priority**

  Lists the power priority (**Low**, **High**, and **Critical**) configured on ports enabled for PoE. (For more information on this topic, see"Configuring PoE Operation" on page K-6.)

- **Alloc by**

  Displays how PoE is allocated (**usage**, **class**, **value**)

- **Alloc Power**

  The maximum amount of PoE power allocated for that port (expressed in watts).Default: 17 watts for PoE; 33 watts for PoE+.

- **Actual Power**

  The power actually being used on that port.

- **Configured Type**

  If configured, shows the user-specified identifier for the port. If not configured, this field is empty.

- **Detection Status**:

  Searching: The port is trying to detect a PD connection.

  Delivering: The port is delivering power to a PD.

  Disabled: On the indicated port, either PoE support is disabled or PoE power is enabled but the PoE module does not have enough power available to supply the port's power needs.

  Fault: The switch detects a problem with the connected PD.

  Other Fault: The switch has detected an internal fault that prevents it from supplying power on that port.

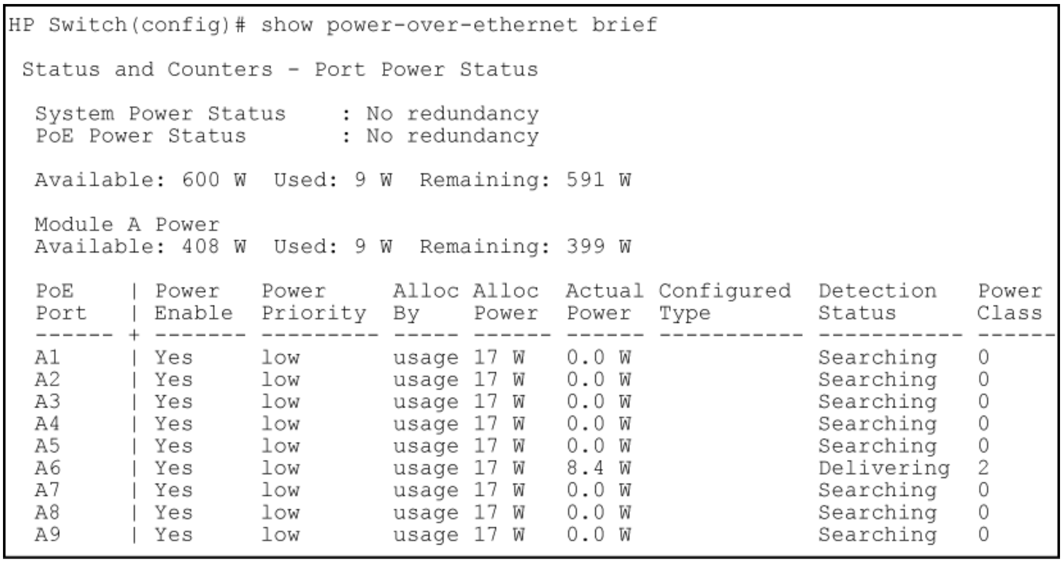
- **Power Class** Shows the 802.3af power class of the PD detected on the indicated port. Classes include:

0	0.44 to 12.95 watts can be drawn by the PD. Default class.
1	0.44 to 3.84 watts
2	3.84 to 6.49 watts
3	6.49 to 12.95 watts
4	For PoE+; up to 25.5 watts can be drawn by the PD

Examples

`show power-over-ethernet brief` displays this output:

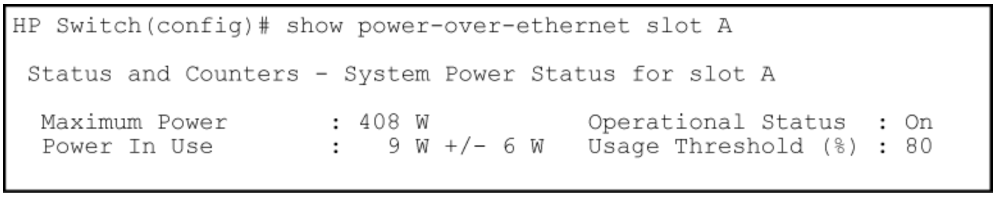
Figure 36 `show power-over-ethernet brief` **command output**



```
HP Switch(config)# show power-over-ethernet brief

 Status and Counters - Port Power Status

  System Power Status     : No redundancy
  PoE Power Status        : No redundancy

  Available: 600 W  Used: 9 W  Remaining: 591 W

  Module A Power
  Available: 408 W  Used: 9 W  Remaining: 399 W

  PoE    | Power   Power     Alloc Alloc  Actual Configured  Detection   Power
  Port   | Enable  Priority  By    Power  Power  Type       Status      Class
  ------ + ------- --------- ----- ------ ------ ----------- ----------- ------
  A1     | Yes     low       usage 17 W   0.0 W              Searching   0
  A2     | Yes     low       usage 17 W   0.0 W              Searching   0
  A3     | Yes     low       usage 17 W   0.0 W              Searching   0
  A4     | Yes     low       usage 17 W   0.0 W              Searching   0
  A5     | Yes     low       usage 17 W   0.0 W              Searching   0
  A6     | Yes     low       usage 17 W   8.4 W              Delivering  2
  A7     | Yes     low       usage 17 W   0.0 W              Searching   0
  A8     | Yes     low       usage 17 W   0.0 W              Searching   0
  A9     | Yes     low       usage 17 W   0.0 W              Searching   0
```

You can also show the PoE information by **slot**:

Figure 37 Showing the PoE information by slot



```
HP Switch(config)# show power-over-ethernet slot A

 Status and Counters - System Power Status for slot A

  Maximum Power        : 408 W          Operational Status  : On
  Power In Use         :   9 W +/- 6 W  Usage Threshold (%) : 80
```

Viewing the PoE status on specific ports

Syntax:

`show power-over-ethernet` *`port-list`*

Displays the following PoE status and statistics (since the last reboot) for each port in *`port-list`*:

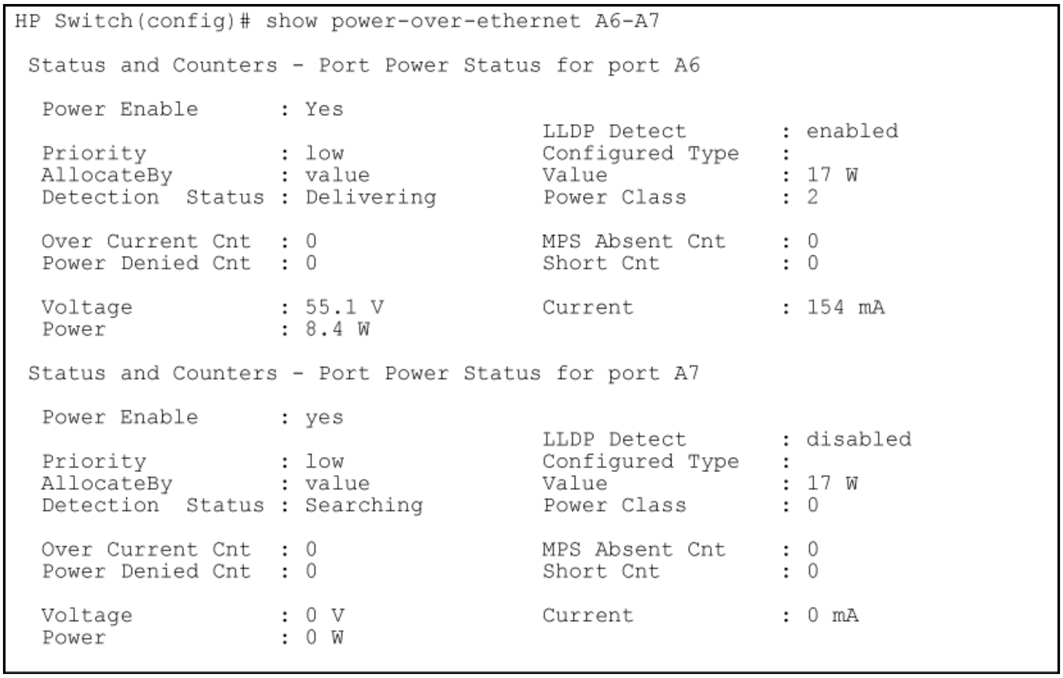
Power Enable	Shows **Yes** for ports enabled to support PoE (the default) and **No** for ports on which PoE is disabled. For ports on which power is disabled, this is the only field displayed by `show power-over-ethernet` *`port-list`*.
Priority	Lists the power priority (**Low**, **High**, and **Critical**) configured on ports enabled for PoE. (For more on this topic, see "Configuring PoE Operation" on page K-6.)
Allocate by	How PoE is allocated (**usage**, **class**, **value**).
Detection Status	Searching — The port is available to support a PD. Delivering — The port is delivering power to a PD. Disabled — PoE power is enabled on the port but the PoE module does not have enough power available to supply the port's power needs. Fault — The switch detects a problem with the connected PD. Other Fault — The switch has detected an internal fault that prevents it from supplying power on that port.

Over Current Cnt	Shows the number of times a connected PD has attempted to draw more than 15.4 watts for PoE or 24.5 watts for PoE+. Each occurrence generates an Event Log message.
Power Denied Cnt	Shows the number of times PDs requesting power on the port have been denied because of insufficient power available. Each occurrence generates an Event Log message.
Voltage	The total voltage, in volts, being delivered to PDs.
Power	The total power, in watts, being delivered to PDs.
LLDP Detect	Port is enabled or disabled for allocating PoE power, based on the link-partner's capabilities via LLDP.
Configured Type	If configured, shows the user-specified identifier for the port. If not configured, the field is empty.
Value	The maximum amount of PoE power allocated for that port (expressed in watts). Default: **17 watts** for PoE; **33 watts** for PoE+
Power Class	Shows the power class of the PD detected on the indicated port. Classes include: 0 0.44 to 12.95 watts 1 0.44 to 3.84 watts 2 3.84 to 6.49 watts 3 6.49 to 12.95 watts 4 For PoE+; up to 25.5 watts can be drawn by the PD
MPS Absent Cnt	Shows the number of times a detected PD has no longer requested power from the port. Each occurrence generates an Event Log message. ("MPS" refers to the "maintenance power signature.")
Short Cnt	Shows the number of times the switch provided insufficient current to a connected PD.
Current	The total current, in mA, being delivered to PDs.

Example

If you want to view the PoE status of ports A6 and A7, you would use **show power-over-ethernet A6-A7** to display the data:

Figure 38 Example of `show power-over-ethernet port-list` output



```
HP Switch(config)# show power-over-ethernet A6-A7

 Status and Counters - Port Power Status for port A6

  Power Enable      : Yes
                                      LLDP Detect       : enabled
  Priority          : low             Configured Type   :
  AllocateBy        : value           Value             : 17 W
  Detection  Status : Delivering      Power Class       : 2

  Over Current Cnt  : 0               MPS Absent Cnt    : 0
  Power Denied Cnt  : 0               Short Cnt         : 0

  Voltage           : 55.1 V          Current           : 154 mA
  Power             : 8.4 W

 Status and Counters - Port Power Status for port A7

  Power Enable      : yes
                                      LLDP Detect       : disabled
  Priority          : low             Configured Type   :
  AllocateBy        : value           Value             : 17 W
  Detection  Status : Searching       Power Class       : 0

  Over Current Cnt  : 0               MPS Absent Cnt    : 0
  Power Denied Cnt  : 0               Short Cnt         : 0

  Voltage           : 0 V             Current           : 0 mA
  Power             : 0 W
```

Planning and implementing a PoE configuration

This section provides an overview of some considerations for planning a PoE application. For additional information on this topic, refer to the *HP PoE Planning and Implementation Guide* which is available on the HP Networking web site at www.hp.com/networking/support.

Some of the elements you may want to consider for a PoE installation include:

- Port assignments to VLANs
- Use of security features
- Power requirements

This section can help you to plan your PoE installation. If you use multiple VLANs in your network, or if you have concerns about network security, you should read the first two topics. If your PoE installation comes close to (or is likely to exceed) the system's ability to supply power to all devices that may request it, then you should also read the third topic. (If it is unlikely that your installation will even approach a full utilization of the PoE power available, then you may find it unnecessary to spend much time on calculating PoE power scenarios.)

Power requirements

To get the best PoE performance, you should provide enough PoE power to exceed the maximum amount of power that is needed by all the PDs that are being used.

By connecting an external power supply you can optionally provision more PoE wattage per port and or supply the switch with redundant 12V power to operate should an internal power supply fail.

By installing a second power supply in the 5406zl/8206zl or a third power supply in a 5412zl/8212zl chassis, depending on how many PoE ports are being supplied with power, the switch can have redundant power if one power supply fails. A Power Supply Shelf (external power supply) can also be connected to the 5400zl/8200zl switches to provide extra or redundant PoE power.

For example, if the 5406zl has two 24-port PoE modules (J8702A) installed, and all ports are using 15.4 watts, then the total wattage used is 739.2 watts (48 x 15.4). To supply the necessary PoE wattage a J8713A power supply is installed in one of the power supply slots.

To gain redundant power, a second J8713A must be installed in the second power supply slot. If the first power supply fails, then the second power supply can supply all necessary power.

See the *HP PoE Planning and Implementation Guide* for detailed information about the PoE/PoE+ power requirements for your switch.

Assigning PoE ports to VLANs

If your network includes VLANs, you may want to assign various PoE-configured ports to specific VLANs. For example, if you are using PoE telephones in your network, you may want to assign ports used for telephone access to a VLAN reserved for telephone traffic.

Applying security features to PoE configurations

You can utilize security features built into the switch to control device or user access to the network through PoE ports in the same way as non-PoE ports.

MAC Address Security: Using Port Security, you can configure each switch port with a unique list of MAC addresses for devices that are authorized to access the network through that port. For more information, refer to the chapter titled “Configuring and Monitoring Port Security” in the Access Security Guide for your switch.

Assigning priority policies to PoE traffic

You can use the configurable QoS (Quality of Service) features in the switch to create prioritization policies for traffic moving through PoE ports. The available classifiers and their order of precedence are show in Table 10 (page 95).

Table 10 Classifiers for prioritizing outbound packets

Priority	QoS classifier
1	UDP/TCP application type (port)
2	Device priority (destination or source IP address)
3	IP type of service (ToS) field (IP packets only)
4	VLAN priority
5	Incoming source-port on the switch
6	Incoming 802.1 priority (present in tagged VLAN environments)

For more on this topic, refer to the chapter titled “Quality of Service: Managing Bandwidth More Effectively” in the *Advanced Traffic Management Guide* for your switch.

About PoE operation

Using the commands described in this chapter, you can:

- Enable or disable PoE operation on individual ports.
- Monitor PoE status and performance per module.
- Configure a non-default power threshold for SNMP and Event Log reporting of PoE consumption on either all PoE ports on the switch or on all PoE ports in one or more PoE modules.
- Specify the port priority you want to use for provisioning PoE power in the event that the PoE resources become oversubscribed.

Power-sourcing equipment (PSE) detects the power needed by a powered device (PD) before supplying that power, a detection phase referred to as "searching." If the PSE cannot supply the required amount of power, it does not supply any power. For PoE using a Type 1 device, a PSE will not supply any power to a PD unless the PSE has at least 17 watts available. For example, if a PSE has a maximum available power of 382 watts and is already supplying 378 watts, and is then connected to a PD requiring 10 watts, the PSE will not supply power to the PD.

For PoE+ using Type 2 devices, the PSE must have at least 33 watts available. A slot in a zl chassis can provide a maximum of 370 watts of PoE/PoE+ power to a module.

Configuration options

In the default configuration, PoE support is enabled on the ports in a PoE module installed on the switch. The default priority for all ports is **low** and the default power notification threshold is **80%**. Using the CLI, you can:

- Disable or re-enable PoE operation on individual PoE ports
- Enable support for pre-standard devices
- Change the PoE priority level on individual PoE ports
- Change the threshold for generating a power level notice
- Manually allocate the amount of PoE power for a port by usage, value, or class
- Allocate PoE power based on the link-partner's capabilities via LLDP

NOTE: The ports support standard networking links and PoE links. You can connect either a non-PoE device or a PD to a port enabled for PoE without reconfiguring the port.

PD support

To best utilize the allocated PoE power, spread your connected PoE devices as evenly as possible across modules. Depending on the amount of power delivered to a PoE module, there may or may not always be enough power available to connect and support PoE operation on all ports in the module. When a new PD connects to a PoE module and the module does not have enough power left for that port, if the new PD connects to a port "X" that has a:

- *Higher* PoEpriority than another port "Y" that is already supporting another PD, the power is removed from port "Y" and delivered to port "X." In this case the PD on port "Y" loses power and the PD on port "X" receives power.
- *Lower* priority than all other PoE ports currently providing power to PDs, power is not supplied to port "X" until one or more PDs using higher priority ports are removed.

In the default configuration (**usage**), when a PD connects to a PoE port and begins operating, the port retains only enough PoE power to support the PD's operation. Unused power becomes available for supporting other PD connections. However, if you configure the `poe-allocate-by` option to either **value** or **class**, all of the power configured is allocated to the port.

For PoE (not PoE+), while 17 watts must be available for a PoE module on the switch to begin supplying power to a port with a PD connected, 17 watts per port is not continually required if the connected PD requires less power. For example, with 20 watts of PoE power remaining available on a module, you can connect one new PD without losing power to any connected PDs on that module. If that PD draws only 3 watts, 17 watts remain available, and you can connect at least one more PD to that module without interrupting power to any other PoE devices connected to the same module. If the next PD you connect draws 5 watts, only 12 watts remain unused. With only 12 unused watts available, if you then connect yet another PD to a higher-priority PoE port, the lowest-priority port on the module loses PoE power and remains unpowered until the module once again has 17 or more watts available. (For information on power priority, see "Power priority operation" (page 97).)

For PoE+, there must be 33 watts available for the module to begin supplying power to a port with a PD connected. A slot in a zl chassis can provide a maximum of 370 watts of PoE/PoE+ power to a module.

Disconnecting a PD from a PoE port makes that power available to any other PoE ports with PDs waiting for power. If the PD demand for power becomes greater than the PoE power available, power is transferred from the lower-priority ports to the higher-priority ports. (Ports not currently providing power to PDs are not affected.)

Power priority operation

If a PSE can provide power for all connected PD demand, it does not use its power priority settings to allocate power. However, if the PD power demand oversubscribes the available power, the power allocation is prioritized to the ports that present a PD power demand. This causes the loss of power from one or more lower-priority ports to meet the power demand on other, higher-priority ports. This operation occurs regardless of the order in which PDs connect to the module's PoE-enabled ports.

Power allocation is prioritized according to the following methods:

- *Priority class* method

  Assigns a power priority of **low** (the default), **high**, or **critical**to each enabled PoE port.

- *Port-number priority* method

  A lower-numbered port has priority over a higher-numbered port within the same configured priority class, for example, port A1 has priority over port A5 if both are configured with **high** priority.

About assigning PoE priority with two or more modules

Ports across two or more modules can be assigned a class priority of low (the default), high, or critical. For example, A5, B7, and C10 could all be assigned a priority class of **Critical**. When power is allocated to the ports on a priority basis, the **Critical** priority power requests are allocated to module A first, then Module B, then C, and so on. Next, the **High** priority power requests are allocated, starting with module A, then B, then C, and the remaining modules in order. Any remaining power is allocated in the same manner for the **Low** priority ports, beginning with module A though the remaining modules. If there is not enough PoE power for all the PDs connected to PoE modules in the switch, power is allocated according to priority class across modules.

Example

All ports on module C are prioritized as **Critical**.

```
HP Switch(config)# interface c1-c24 power-over-ethernet
    critical
```

All ports on module A are prioritized as **Low**.

```
HP Switch(config)# interface a1-a24 power-over-ethernet
    low
```

There are 48 PDs attached to all ports of modules A and C (24 ports each module); however, there is enough PoE power for only 32 ports (8.5 watts × 32 ports=273 watts). The result is that all the **Critical** priority ports on module C receive power, but only 8 ports on module A receive power.

On module A, the port A1 has the highest priority of the ports in that module if all ports are in the same priority class, which is the case for this example. Since a minimum 17 + 5 watts of power is allocated per PoE module for PoE, port A1 will always receive PoE power. If another port on module A had a higher priority class than port A1, that port would be allocated the power before port A1.

For PoE+ modules there must be a minimum of 33 + 5 watts of power allocated per PoE+ module.

About configuring PoE operation

In thedefault configuration,PoE support is enabled on the ports in a PoE module installed on the switch. The default priority for all ports is **low** and the default power notification threshold is **80%**.

Using the CLI, you can:

- Disable or re-enable PoE operation on individual PoE ports.
- Enable support for pre-standard devices.
- Change PoE priority level on individual PoE ports.
- Change the threshold for generating a power level notice.
- Manually allocate the amount of PoE power for a port by usage, value, or class.
- Allocate PoE power based on the link-partner's capabilities via LLDP.

For a given level, ports are prioritized by port number in ascending order. For example, if ports A1 to A24 have a priority level of critical, port A1 has priority over ports A2 to A24.

If there is not enough power available to provision all active PoE ports at a given priority level, the lowest-numbered port at that level is provisioned first. For chassis switches, the lowest-numbered port at that level starting with module A, then B, C, and so on is provisioned. PoE priorities are invoked only when all active PoE ports cannot be provisioned (supplied with PoE power).

In chassis switches, you can use one command to set the same priority level on PoE ports in multiple modules. For example, to configure the priority to **High** for ports c5 to c10, C23 to C24, D1 to D10, and D12, you could use this command:

```
HP Switch(config)# interface c5-c10,c23-c24,
d1-d10,d12 power-over-ethernet high
```

Example

Suppose that you configure the PoE priority for a module in slot C as shown in Table 11 (page 98).

Table 11 PoE priority operation on a PoE module

Port	Priority setting	Configuration command[1] and resulting operation with PDs connected to ports C3 through C24
C3 - C17	**Critical**	In this example, the following CLI command sets ports C3 to C17 to **Critical**: `HP Switch(config)# interface c3-c17 power-over-ethernet critical` The **critical** priority class always receives power. If there is not enough power to provision PDs on all ports configured for this class, no power goes to ports configured for **high** and **low** priority. If there is enough power to provision PDs on only some of the critical-priority ports, power is allocated to these ports in ascending order, beginning with the lowest-numbered port in the class, which, in this case, is port 3.
C18 - C21	**high**	In this example, the following CLI command sets ports C19 to C22 to **high**: `HP Switch(config)# interface c19-c22 power-over-ethernet high` The **high** priority class receives power only if all PDs on ports with a **critical** priority setting are receiving power. If there is not enough power to provision PDs on all ports with a **high** priority, no power goes to ports with a low priority. If there is enough power to provision PDs on only some of the

Table 11 PoE priority operation on a PoE module *(continued)*

Port	Priority setting	Configuration command[1] and resulting operation with PDs connected to ports C3 through C24
		high-priority ports, power is allocated to these ports in ascending order, beginning, in this example, with port 18, until all available power is in use.
C22 - C24	**low**	In this example, the CLI command sets ports C23 to C24 to **low**[2]: `HP Switch(config)# interface c23-c24 power-over-ethernet low` This priority class receives power only if all PDs on ports with **high** and **critical** priority settings are receiving power. If there is enough power to provision PDs on only some low-priority ports, power is allocated to the ports in ascending order, beginning with the lowest-numbered port in the class (port 22, in this case), until all available power is in use.
C1 - C2	*N/A*	In this example, the CLI command disables PoE power on ports C1 to C2: `HP Switch(config)# no interface c1-c2 power-over-ethernet` There is no priority setting for the ports in this example.

[1] For a listing of PoE configuration commands with descriptions, see "Configuring PoE Operation" on page K-6.

[2] In the default PoE configuration, the ports are already set to **low** priority. In this case, the command is not necessary.

About configuring thresholds for generating a power notice

You can configure one of the following thresholds:

A global power threshold that applies to all modules on the switch.

This setting acts as a trigger for sending a notice when the PoE power consumption on any PoE module installed in the switch crosses the configured global threshold level. (Crossing the threshold level in either direction—PoE power usage either increasing or decreasing—triggers the notice.) The default setting is 80%.

A per-slot power threshold that applies to an individual PoE module installed in the designated slot.

This setting acts as a trigger for sending a notice when the module in the specified slot exceeds or goes below a specific level of PoE power consumption.

Example

Suppose slots A, B, and C each have a PoE module installed. In this case, executing the following command sets the global notification threshold to 70% of available PoE power.

```
HP Switch(config)# power-over-ethernet threshold
       70
```

With this setting, if module B is allocated 100 watts of PoE power and is using 68 watts, and then another PD is connected to the module in slot B that uses 8 watts, the 70% threshold of 70 watts is exceeded. The switch sends an SNMP trap and generates this Event Log message:

```
Slot B POE usage has exceeded threshold of 70%.
```

If the switch is configured for debug logging, it also sends the Event Log message to the configured debug destinations.

On any PoE module, if an increasing PoE power load (1) exceeds the configured power threshold—which triggers the log message and SNMP trap—and then (2) later decreases and drops below the threshold again, the switch generates another SNMP trap, plus a message to the Event Log and any configured Debug destinations.

Example

To continue the preceding example, if the PoE power usage on the PoE module in slot B drops below 70%, another SNMP trap is generated and you will see this message in the Event Log:

```
Slot B POE usage is below threshold of 70%.
```

By using the `[slot` *`slot-id-range`*`]` option, you can specify different notification thresholds for different PoE modules installed in the switch. For example, you could set the power threshold for a PoE module in slot "A" to 75% and the threshold for the module in slot "B" to 68% by executing the following two commands:

```
HP Switch(config)# power-over-ethernet slot a
  threshold 75
HP Switch(config)# power-over-ethernet slot b
  threshold 68
```

The last `threshold` command affecting a given slot supersedes the previous threshold command affecting the same slot. Thus, executing the following two commands in the order shown sets the threshold for the PoE module in slot "D" to 75%, but leaves the thresholds for any PoE modules in the other slots at 90%:

```
HP Switch(config)# power-over-ethernet
  threshold 90
HP Switch(config)# power-over-ethernet slot d
  threshold 75
```

(If you reverse the order of the above two commands, all PoE modules in the switch will have a threshold of 90%.)

Without the `[slot` *`slot-id-range`*`]` option, the switch applies one power threshold setting on all PoE modules installed in the switch.

About PoE/PoE+ allocation using LLDP information

LLDP with PoE

When using PoE, enabling `poe-lldp-detect` allows automatic power configuration if the link partner supports PoE. When LLDP is enabled, the information about the power usage of the PD is available, and the switch can then comply with or ignore this information. You can configure PoE on each port according to the PD (IP phone, wireless device, and so on) specified in the LLDP field. The default configuration is for PoE information to be ignored if detected through LLDP.

NOTE: Detecting PoE information via LLDP affects only power delivery; it does not affect normal Ethernet connectivity.

LLDP with PoE+

Overview

The DLC for PoE provides more exact control over the power requirement between a PSE and PD. The DLC works in conjunction with the PLC and is mandatory for any Type-2 PD that requires more than 12.95 watts of input power.

NOTE: DLC is defined as part of the IEEE 802.3at standard.

You can implement the power negotiation between a PSE and a PD at the physical layer or at the data link layer. After the link is powered at the physical layer, the PSE can use LLDP to query the PD repeatedly to discover the power needs of the PD. Communication over the data link layer allows finer control of power allotment, which makes it possible for the PSE to supply dynamically the power levels needed by the PD. Using LLDP is optional for the PSE but mandatory for a Type 2 PD that requires more than 12.95 watts of power.

If the power needed by the PD is not available, that port is shut off.

PoE allocation

There are two ways LLDP can negotiate power with a PD:

- Using LLDP MED TLVs

  Disabled by default. Can be enabled using the
  `int` *`port-list`* `PoE-lldp-detect [ enabled | disabled ]`
  command, as shown below.

  LLDP MED TLVs sent by the PD are used to negotiate power only if the LLDP PoE+ TLV is disabled or inactive; if the LLDP PoE+ TLV is sent as well (not likely), the LLDP MED TLV is ignored.

- Using LLDP PoE+ TLVs

  Enabled by default. The LLDP PoE+ TLV is always advertised unless it has been disabled (enable it by using the `lldp config` *`port-list`* `dot3TlvEnable poeplus_config` command).

  For the command syntax, see "Initiating advertisement of PoE+ TLVs" (page 87). It always takes precedence over the LLDP MED TLV.

Enabling `PoE-lldp-detect` allows the data link layer to be used for power negotiation.When a PD requests power on a PoE port, LLDP interacts with PoE to see if there is enough power to fulfill the request. Power is set at the level requested. If the PD goes into power-saving mode, the power supplied is reduced; if the need for power increases, the amount supplied is increased. PoE and LLDP interact to meet the current power demands.

Operation Note

The advertisement of power with TLVs for LLDP PoE+ is enabled by default. If LLDP is disabled at runtime and a PD is using PoE+ power that has been negotiated through LLDP, there will be a temporary power drop. The port will begin using PoE+ power through the PLC. This event is recorded in the event log. An example message would look like the following:

```
W 08/04/10 13:35:50 02768 ports: Port A1 PoE power dropped. Exceeded physical classification for a PoE Type1
device (LLDP process disabled)
```

When LLDP is enabled again, it causes a temporary power drop. This event is also recorded in the event log. An example message looks like the following:

```
W 08/04/10 13:36:31 02771 ports: Port A1 PoE power dropped. Exceeded physical classification due to change in
classification type (LLDP process enabled)
```

5 Port Trunking

Table 12 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
`show trunks`	Lists static trunk type and group for all ports or for selected ports	-	(page 103)	(page 107)
`show lacp`	Lists data for only the LACP-configured ports	-	(page 104)	-
`trunk port-list trk1 ... trk144 [[trunk] | lacp ]`	Configures the specified static trunk type.	trunk	(page 104)	(page 107)
`no trunk` *`port-list`*	Removes the specified ports from an existing trunk group	-	(page 105)	-
`interface` *`port-list`* `lacp active`	Configures *`port-list`* as LACP active.	-	(page 105)	-
`no interface` *`port-list`* `lacp`	Removes `port-list` from any dynamic LACP trunk and returns the ports in `port-list` to passive LACP	-	(page 105)	-
`trunk-load-balance L3-based | L4-based`	Enables load balancing based on Layer 4 information if it is present.	L3-based load balancing	(page 108)	-
`switch-interconnect port-num | trk1...trkN`	Configures an InterSwitch-Connection (ISC) port.	-	(page 110)	-

`trunk` *`port-list`* `[ trk1 | trk2 ... trkN ][ trunk | lacp | dt-lacp | dt-trunk ]`
`no trunk` *`port-list`*
	Configures distributed trunking on a switch.	-	(page 110)	-

`[no] distributed-trunking [hold-timer3-10] [ peer-keepalive destination ip-address | vlan vid [interval 400-10000] [ timeout 3-20] [udp-port` *`1024-49151`*`] ]`	Configures the peer-keepalive parameters for distributed trunking	see "Configuring peer-keepalive links" (page 111) for parameter defaults	(page 111)	-
`show lacp [distributed]`	Displays information about distributed trunks and LACP status	-	"Viewing distributed trunking information" (page 111)	-

Table 12 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`show distributed-trunking peer-keepalive`	Displays information about peer-keepalive parameters	-	"Viewing information about the peer-keepalive configuration" (page 112)	-
`show switch-interconnect`	Displays information about switch interconnect settings	-	"Viewing the switch interconnect information" (page 113)	-

CAUTION: To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports you want to add to or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

Viewing and configuring port trunk groups (CLI)

You can list the trunk type and group for all ports on the switch or for selected ports. You can also list LACP-only status information for LACP-configured ports.

Viewing static trunk type and group for all ports or for selected ports

Syntax:

```
show trunks [ port-list ]
```

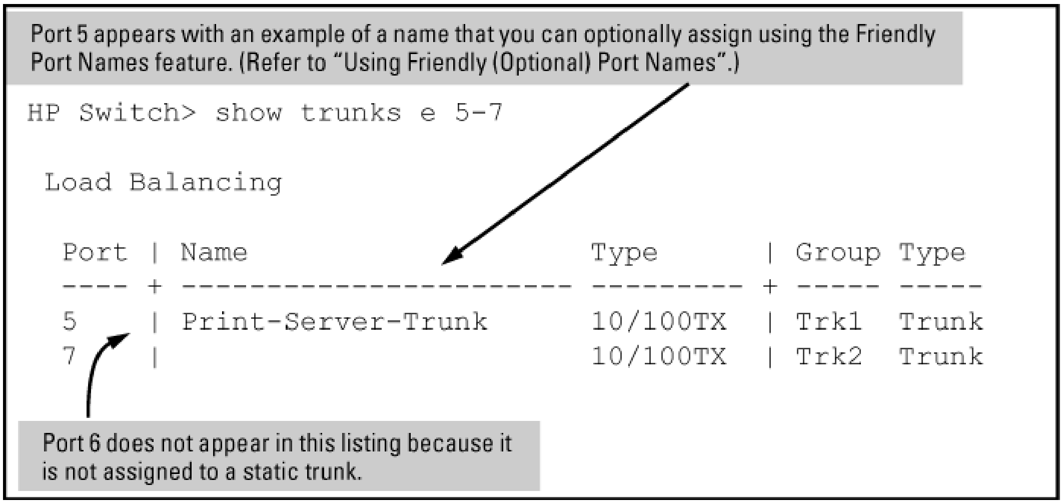
Omitting the `port-list` parameter results in a static trunk data listing for all LAN ports in the switch.

Example

In a switch where ports A4 and A5 belong to Trunk 1 and ports A7 and A8 belong to Trunk 2, you have the options shown in figures Figure 39 (page 103) and Example 33 (page 104) for displaying port data for ports belonging to static trunks.

Using a port list specifies, for switch ports in a static trunk group, only the ports you want to view. In this case, the command specifies ports A5 through A7. However, because port A6 is not in a static trunk group, it does not appear in the resulting listing:

Figure 39 Example listing specific ports belonging to static trunks



Port 5 appears with an example of a name that you can optionally assign using the Friendly Port Names feature. (Refer to "Using Friendly (Optional) Port Names".)

```
HP Switch> show trunks e 5-7

 Load Balancing

  Port | Name                    Type      | Group Type
  ---- + ----------------------- --------- + ----- -----
  5    | Print-Server-Trunk      10/100TX  | Trk1  Trunk
  7    |                         10/100TX  | Trk2  Trunk
```

Port 6 does not appear in this listing because it is not assigned to a static trunk.

The `show trunks port-list` command in the above example includes a port list, and thus shows trunk group information only for specific ports that have membership in a static trunk. In Example 33 (page 104), the command does not include a port list, so the switch lists all ports having static trunk membership.

Example 33 Example of a show trunk listing without specifying ports

```
HP Switch> show trunks

 Load Balancing

 Port | Name                    Type      | Group Type
 ---- + ----------------------- --------- + ----- -----
 4    | Print-Server-Trunk      10/100TX  | Trk1  Trunk
 5    | Print-Server-Trunk      10/100TX  | Trk1  Trunk
 7    |                         10/100TX  | Trk2  Trunk
 8    |                         10/100TX  | Trk2  Trunk
```

Viewing static LACP and dynamic LACP trunk data

Syntax:

`show lacp`

Lists data for only the LACP-configured ports.

Example

Ports A1 and A2 have been previously configured for a static LACP trunk. (For more on the `Active` parameter, see Table 16 (page 125).)

Example 34 Example of a show LACP listing

```
HP Switch> show lacp

                            LACP
       LACP     Trunk    Port                LACP     Admin  Oper
Port   Enabled  Group    Status   Partner  Status   Key    Key
----   -------  -------  -------  -------  -------  ------ ------
Al     Active   Trkl     Up       Yes      Success  0      250
A2     Active   Trkl     Up       Yes      Success  0      250
A3     Active   A3       Down     No       Success  0      300
A4     Passive  A4       Down     No       Success  0      0
A5     Passive  A5       Down     No       Success  0      0
A6     Passive  A6       Down     No       Success  0      0
```

For a description of each of the above-listed data types, see Table 16 (page 125).

Configuring a static trunk or static LACP trunk group

IMPORTANT: Configure port trunking before you connect the trunked links between switches. Otherwise, a broadcast storm could occur. (If you need to connect the ports before configuring them for trunking, you can temporarily disable the ports until the trunk is configured. See "Enabling_or_Disabling_Ports_and_Configuring_Port_Mode".)

Syntax:

`trunk  port-list trk1 ... trk144  trunk | lacp`

Configures the specified static trunk type.

Example

This example uses ports C4 to C6 to create a non-protocol static trunk group with the group name Trk2.

```
HP Switch(config)# trunk c4-c6 trk2 trunk
```

Removing ports from a static trunk group

△ **CAUTION:** Removing a port from a trunk can create a loop and cause a broadcast storm. When you remove a port from a trunk where spanning tree is not in use, HP Switch recommends that you first disable the port or disconnect the link on that port.

Syntax:

`no trunk` *`port-list`*

Removes the specified ports from an existing trunk group.

Example

To remove ports C4 and C5 from an existing trunk group:

```
HP Switch(config)# no trunk c4-c5
```

Enabling dynamic LACP trunk groups

An individual trunk can have up to eight links, with additional standby links if you are using LACP. You can configure trunk group types as follows:

Syntax:

`interface` *`port-list`* `lacp active`

Configures `port-list` as LACP active. If the ports at the other end of the links on `port-list` are configured as LACP passive, this command enables a dynamic LACP trunk group on `port-list` .

Example

This example uses ports C4 and C5 to enable a dynamic LACP trunk group.

```
HP Switch(config)# interface c4-c5 lacp active
```

Removing ports from a dynamic LACP trunk group

To remove a port from dynamic LACP trunk operation, you must turn off LACP on the port. (On a port in an operating, dynamic LACP trunk, you cannot change between LACP `Active` and LACP `passive` without first removing LACP operation from the port.)

△ **CAUTION:** Unless spanning tree is running on your network, removing a port from a trunk can result in a loop. To help prevent a broadcast storm when you remove a port from a trunk where spanning tree is not in use, HP recommends that you first disable the port or disconnect the link on that port.

Syntax:

`no interface` *`port-list`* `lacp`

Removes `port-list` from any dynamic LACP trunk and returns the ports in `port-list` to passive LACP.

Example

Port C6 belongs to an operating, dynamic LACP trunk. To remove port C6 from the dynamic trunk and return it to passive LACP, do the following:

```
HP Switch(config)# no interface c6 lacp
HP Switch(config)# interface c6 lacp passive
```

In the above example, if the port on the other end of the link is configured for active LACP or static LACP, the trunked link will be re-established almost immediately.

Setting the LACP key

During dynamic link aggregation using LACP, ports with the same key are aggregated as a single trunk.

Syntax:

[no]`lacp [[active] | [passive] | [key 0-65535]]`

Example 35 Enabling LACP and configuring an LACP key

```
HP Switch(config)# int A2-A3 lacp active
HP Switch(config)# int A2-A3 lacp key 500

HP Switch(config)# show lacp

                                 LACP

         LACP      Trunk    Port               LACP     Admin  Oper
  Port   Enabled   Group    Status   Partner   Status   Key    Key
  ----   -------   -------  -------  -------   -------  ------ ------
  A2     Active    A2       Down     No        Success  500    500
  A3     Active    A3       Down     No        Success  500    500
```

Example 36 Interface configured with a different LACP key

```
HP Switch(config)# int A5 lacp active
HP Switch(config)# int A5 lacp key 250

HP Switch> show lacp

LACP

      LACP      Trunk     Port              LACP      Admin  Oper
Port  Enabled   Group     Status   Partner  Status    Key    Key
----  -------   -------   -------  -------  -------   ------ ------
Al    Active    Dyn1      Up       Yes      Success   100    100
A2    Active    Dyn1      Up       Yes      Success   100    100
A3    Active    Dyn1      Up       Yes      Success   100    100
A4    Active    Dyn1      Up       Yes      Success   100    100
A5    Active    A5        Up       No       Success   250    250
```

Viewing existing port trunk groups (WebAgent)

While the WebAgent does not enable you to configure a port trunk group, it does provide a view of an existing trunk group.

To view any port trunk groups:

1. In the navigation pane, click **Interface**.
2. Click **Port Info/Config**. The trunk information for the port displays in the **Port Properties** box.

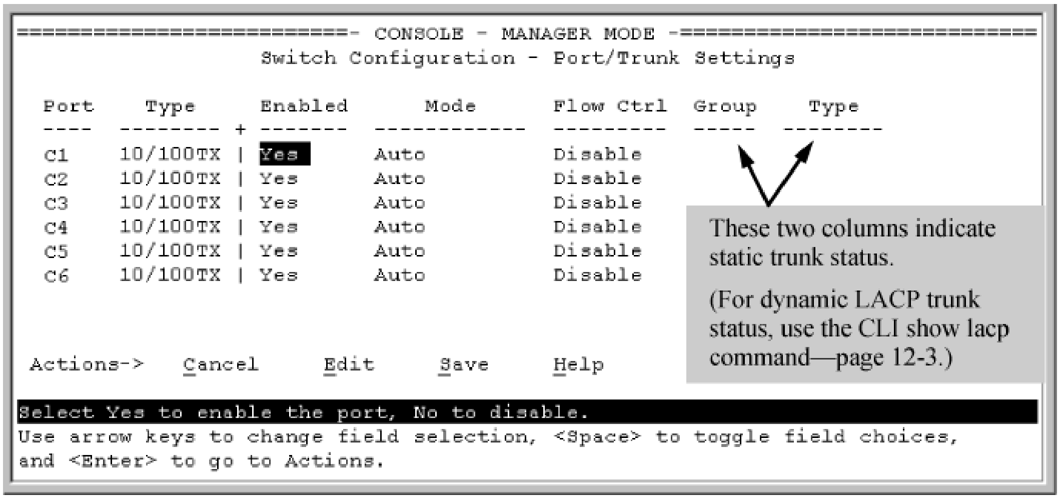
Viewing and configuring a static trunk group (Menu)

IMPORTANT: Configure port trunking *before* you connect the trunked links to another switch, routing switch, or server. Otherwise, a broadcast storm could occur. (If you need to connect the ports before configuring them for trunking, you can temporarily disable the ports until the trunk is configured. See "Enabling or Disabling Ports and Configuring Port_Mode".)

This procedure uses the Port/Trunk Settings screen to configure a static port trunk group on the switch.

1. Follow the procedures in the preceding IMPORTANT note.
2. From the Main Menu, select:
   2. Switch Configuration …
   2. Port/Trunk Settings
3. Press **[E]** (for `Edit`) and then use the arrow keys to access the port trunk parameters.

Figure 40 Example of the menu screen for configuring a port trunk group



```
==========================- CONSOLE - MANAGER MODE -============================
                  Switch Configuration - Port/Trunk Settings

  Port     Type      Enabled      Mode          Flow Ctrl  Group    Type
  ----   --------- + -------  ------------     ---------  -----  --------
  C1     10/100TX  | Yes      Auto             Disable
  C2     10/100TX  | Yes      Auto             Disable
  C3     10/100TX  | Yes      Auto             Disable
  C4     10/100TX  | Yes      Auto             Disable
  C5     10/100TX  | Yes      Auto             Disable
  C6     10/100TX  | Yes      Auto             Disable



 Actions->    Cancel     Edit     Save     Help

Select Yes to enable the port, No to disable.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

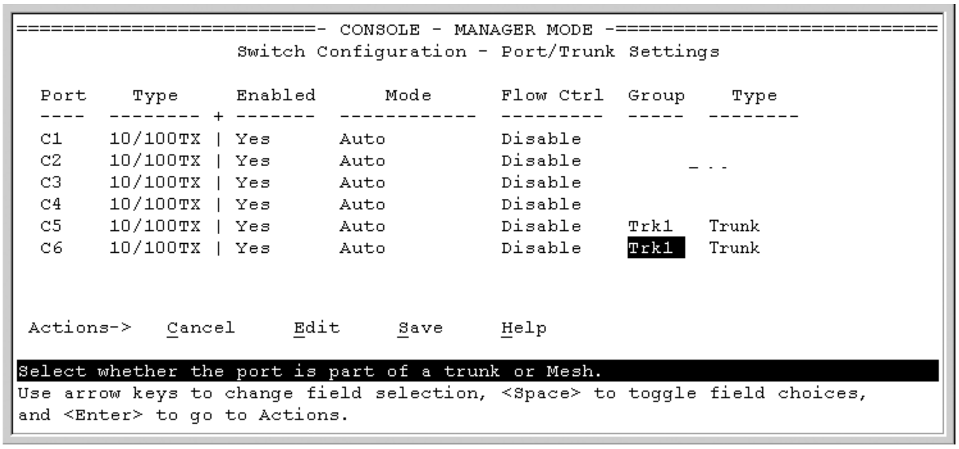
These two columns indicate static trunk status.

(For dynamic LACP trunk status, use the CLI show lacp command—page 12-3.)

4. In the Group column, move the cursor to the port you want to configure.
5. Use the Space bar to choose a trunk group assignment (`Trk1`, `Trk2`, and so on) for the selected port.
   - For proper trunk operation, all ports in a trunk must have the same media type and mode (such as 10/100TX set to 100FDx, or 100FX set to 100FDx). The flow control settings must also be the same for all ports in a given trunk. To verify these settings, see"Viewing Port Status and Configuring Port Parameters".
   - You can configure the trunk group with up to eight ports per trunk. If multiple VLANs are configured, all ports within a trunk will be assigned to the same VLAN or set of VLANs. (With the 802.1Q VLAN capability built into the switch, more than one VLAN can be assigned to a trunk. See the chapter "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.)

     (To return a port to a non-trunk status, keep pressing the Space bar until a blank appears in the highlighted Group value for that port.)

Figure 41 Example of the Configuration for a Two-Port Trunk Group



```
==========================- CONSOLE - MANAGER MODE -============================
                   Switch Configuration - Port/Trunk Settings

  Port    Type      Enabled      Mode        Flow Ctrl  Group   Type
  ----  --------- + -------  ------------  ---------  -----  --------
  C1    10/100TX  | Yes      Auto          Disable
  C2    10/100TX  | Yes      Auto          Disable              _ . .
  C3    10/100TX  | Yes      Auto          Disable
  C4    10/100TX  | Yes      Auto          Disable
  C5    10/100TX  | Yes      Auto          Disable    Trk1   Trunk
  C6    10/100TX  | Yes      Auto          Disable    Trk1   Trunk


 Actions->   Cancel     Edit     Save     Help

Select whether the port is part of a trunk or Mesh.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

6. Move the cursor to the Type column for the selected port and use the Space bar to select the trunk type:
   - LACP
   - Trunk (the default type if you do not specify a type)

   All ports in the same trunk group on the same switch must have the same Type (`LACP` or `Trunk`).
7. When you are finished assigning ports to the trunk group, press **[Enter]**, then **[S]** (for `Save`) and return to the Main Menu. (It is not necessary to reboot the switch.)

   During the Save process, traffic on the ports configured for trunking is delayed for several seconds. If the Spanning Tree Protocol is enabled, the delay may be up to 30 seconds.
8. Connect the trunked ports on the switch to the corresponding ports on the opposite device. If you previously disabled any of the trunked ports on the switch, enable them now. (See "Viewing Port Status and Configuring Port Parameters")

Check the Event Log ("Using the Event Log for Troubleshooting Switch Problems" on page C-28) to verify that the trunked ports are operating properly.

Enabling L4-based trunk load balancing (CLI)

For detailed information about trunk load balancing, see "Trunk load balancing using Layer 4 ports" (page 130).

Enter the following command with the `L4-based` option to enable load balancing on Layer 4 information when it is present.

Syntax:

```
trunk-load-balance [  L3-based   | L4-based ]
```

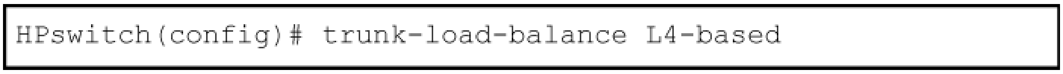
When the`L4-based` option is configured, enables load balancing based on Layer 4 information if it is present. If it is not present, Layer 3 information is used if present; if Layer 3 information is not present, Layer 2 information is used. The configuration is executed in global configuration context and applies to the entire switch.

`L3-based`	Load balance on Layer 3 information if present, or Layer 2 information.
`L4-based`	Load balance on Layer 4 port information if present, or Layer 3 if present, or Layer 2.

Default: L3-based load balancing

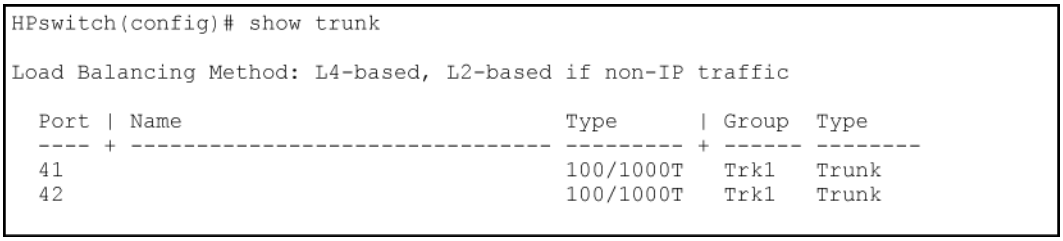
Examples

Figure 42 Enabling L4-based trunk load balancing



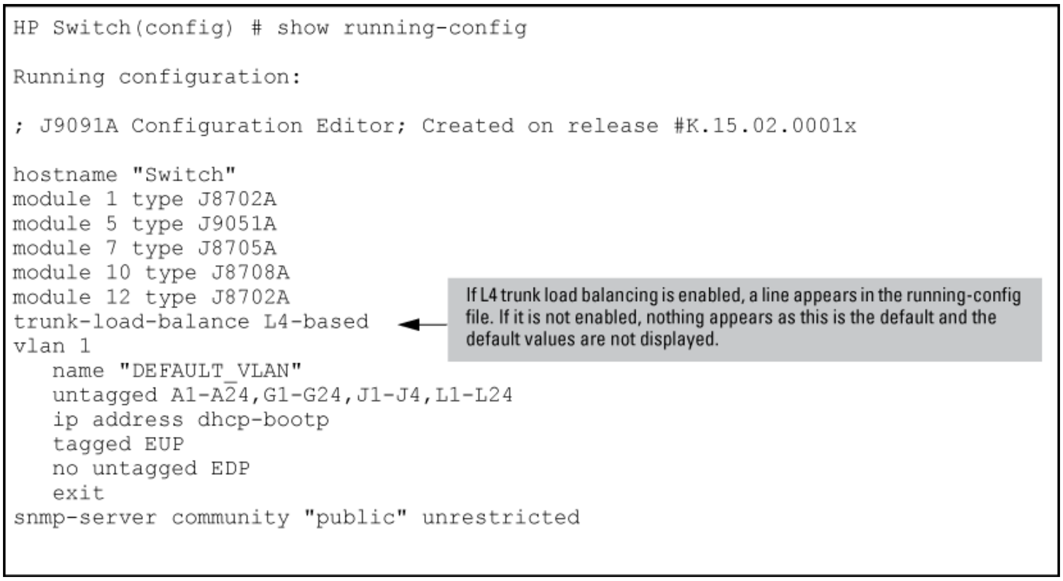
```
HPswitch(config)# trunk-load-balance L4-based
```

Figure 43 Output when L4-based trunk load balancing is enabled



```
HPswitch(config)# show trunk

Load Balancing Method: L4-based, L2-based if non-IP traffic

  Port | Name                             Type      | Group  Type
  ---- + -------------------------------- --------- + ------ --------
  41                                      100/1000T   Trk1   Trunk
  42                                      100/1000T   Trk1   Trunk
```

Figure 44 Running config file when L4-based trunk load balancing is enabled



```
HP Switch(config) # show running-config

Running configuration:

; J9091A Configuration Editor; Created on release #K.15.02.0001x

hostname "Switch"
module 1 type J8702A
module 5 type J9051A
module 7 type J8705A
module 10 type J8708A
module 12 type J8702A
trunk-load-balance L4-based
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A24,G1-G24,J1-J4,L1-L24
   ip address dhcp-bootp
   tagged EUP
   no untagged EDP
   exit
snmp-server community "public" unrestricted
```

If L4 trunk load balancing is enabled, a line appears in the running-config file. If it is not enabled, nothing appears as this is the default and the default values are not displayed.

Displaying information about trunk load balancing

The show trunks load-balance interface command displays the port on which the information will be forwarded out for the specified traffic flow with the specified source and destination address.

Syntax:

`show trunks load-balance interface` *`trunk-id`* `mac` *`src-addr dest-addr`* `[ip` *`src-addr dest-addr`* `[[`*`src-tcp-port`*`] | [`*`src-upd-port`*`] [[`*`dest-tcp-port`*`] | [`*`dest-udp-port`*`]]]]`
`inbound-port` *`port-num`*

Displays the port on which the information will be forwarded out for the specified traffic flow with the specified source and destination address.

`trunk-id` The trunk id (trk1, trk2, etc).

`mac` *`src-addr dest-addr`* The source MAC address and the destination MAC address.

`ip` *`src-addr dest-addr`* The source IPv4 /IPv6 address and the destination IPv4/IPv6 address.

`[`*`src-tcp-port`*`|`*`src-udp-port`*`]` The source TCP port or the source UDP port.

[*dest-tcp-port*|*dest-udp-port*] The destination TCP port or the destination UDP port.

`inbound-port` *port-num* the port number of which the traffic is received.

Example 37 Example showing information about the forwarding port

```
HP Switch# show trunks load-balance interface trk1 mac 424521-498421 534516-
795463 inbound-port a5
Traffic in this flow will be forwarded out port 23 based on the confiugred L2
load balancing.
```

Operating notes

The port cannot be determined if:

- All the ports in the trunk are down.
- The MAC address is all zeros.
- The source MAC address is broadcast or multicast.

Distributed trunking

For detailed information on distributed trunking, see "Distributed trunking overview" (page 131).

Configuring ISC ports

You must configure the ISC ports before you can configure the trunks for distributed trunking.

Syntax:

```
switch-interconnect[  port-num | trk1...trkN  ]
no switch-interconnect
```

Configures an InterSwitch-Connection (ISC) port. The `[  port-num | trk1...trkN ]` variable is the interconnect interface that connects two distributed trunking switches. It can be a physical port, manual LACP trunk, or manual non-protocol trunk. You can override an ISC configuration by configuring the command with a different value.

The `no` form of the command removes the ISC interface configuration.

NOTE: A port that is already part of a trunk cannot be configured as an ISC interface.

Configuring distributed trunking ports

Distributed trunking ports must be configured manually.

Syntax:

`trunk` *port-list* `trk1 | trk2 ... trkN [ trunk | lacp | dt-lacp | dt-trunk ]`
`no trunk` *port-list*

Configures distributed trunking on a switch. Use either the `dt-lacp` or`dt-trunk` option.

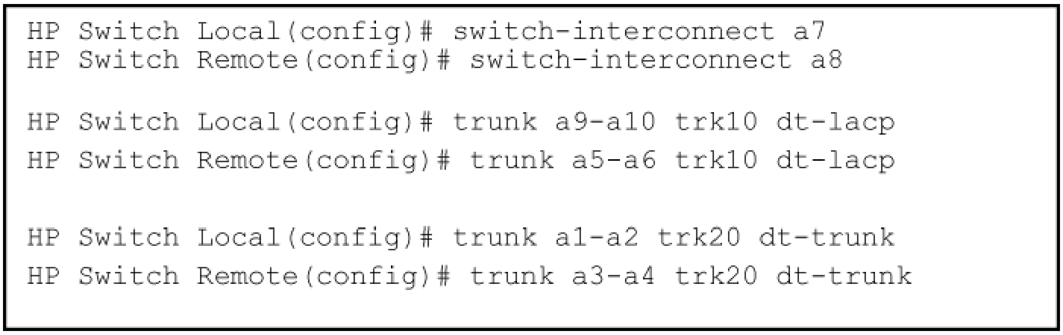
The trunk groups and trunk types must be identical in both switches. For example, if Switch Local is configured with `trk1`and uses the `dt-lacp` option, Switch Remote also must be configured with `trk1` and use the `dt-lacp`option to form a distributed trunk. Similarly, if Switch Local is configured with `trk2` and uses the `dt-trunk` option, Switch Remote must be configured with `trk2` and use the `dt-trunk` option to form the distributed trunk.

The `no` form of the command removes the distributed trunking configuration on the switch.

Example

Figure 45 (page 111) shows an ISC port being configured for the local switch and the remote switch.

Figure 45 Configuring distributed trunking



```
HP Switch Local(config)# switch-interconnect a7
HP Switch Remote(config)# switch-interconnect a8

HP Switch Local(config)# trunk a9-a10 trk10 dt-lacp
HP Switch Remote(config)# trunk a5-a6 trk10 dt-lacp

HP Switch Local(config)# trunk a1-a2 trk20 dt-trunk
HP Switch Remote(config)# trunk a3-a4 trk20 dt-trunk
```

Configuring peer-keepalive links

For detailed information about configuring peer-keepalive links, see "About configuring peer-keepalive links" (page 133).

Syntax:

`[no] distributed-trunking [hold-timer3-10] [ peer-keepalive destination ip-address  | vlan vid [interval 400-10000] [ timeout 3-20] [udp-port` *`1024-49151`*`] ]`

Distributed trunking uses a VLAN interface between DT peers to transmit periodic peer-keepalive messages. This command configures the peer-keepalive parameters for distributed trunking.

`hold-timer 3-10`	Configures the hold time in seconds. Default is 3 seconds.
`peer-keepalive:`	
	`destination`: The destination IPv4 address to be used by DT switches to send peer-keepalive messages to the peer DT switch when the ISC is down.
	`vlan` *`vid`* : The VLAN used exclusively for sending and receiving peer-keepalive messages.
	`interval 400-10000:` The interval between peer-keepalive messages (in milliseconds). Default is 1000 milliseconds.
	`timeout 3-20:` The peer-keepalive timeout in seconds. Default is 5 seconds.
	`udp-port 1024-49151:` The source UDP port to be used for transmitting peer-keepalive HELLO messages.

Viewing distributed trunking information

Syntax:

`show lacp [distributed]`

Displays information about distributed trunks and LACP status.

Example

```
HP Switch Local (config)#: show lacp distributed
                              Distributed LACP
Local Port Status:

         LACP        Trunk      Port                  LACP     Admin     Oper
Port     Enabled     Group      Status     Partner    Status   Key       Key
-----   ---------   -------   ---------   ---------   ------  -------    ---A9      Active     Trk10
  Up        Yes         Sucess    350      350A10     Active     Trk10       Up         Yes        Sucess
  350      350

Remote Port Status
         LACP        Trunk      Port                  LACP     Oper
Port     Enabled     Group      Status     Partner    Status   Key
-----   ---------   -------   ---------   ---------   ------   -----
A5       Active      Trk10      Up          Yes       Sucess     200
A6       Active      Trk10      Up          Yes       Sucess     200
```

Syntax

```
show distributed trunk consistency parameters global
```

This command displays configured features on VLANs that have dt-lacp or dt-trunk ports as member port. This command also displays VLAN memberships and loop-protect status of a given DT trunk. You can use this command to determine if there is any mismatch in the configuration parameters on VLANs configured for DT ports or on DT interfaces.

Example

```
show distributed trunk consistency parameters global

                              Local             Peer

Image Version                 K.15.XX           K.15.XX
IP Routing                    Enabled           Enabled
Peer keepalive interval (ms)  1000              1000

IGMP enabled VLANs on Local : 1 10, 100 110, 501 ,600
610 ,800
IGMP enabled VLANs on Peer : 1 10, 100 110, 501 ,600

DHCP snooping enabled VLANs on Local : 1,2
DHCP snooping enabled VLANs on Peer : 1

Loop protect enabled VLANs on Local : 1,4
Loop protect enabled VLANs on Peer : 1,5

MLD enabled VLANs on Local : 1 10
MLD enabled VLANs on Peer : 1 10
```

Example

```
Show distributed trunk
consistency parameters trunk <trk1...trkN>
Allowed VLANs on Local : 1 10, 100 110, 501 ,600
610 ,800
Allowed VLANs on Peer : 1 10, 100 110, 501 ,600
610 ,800

Name            Local Value             Peer Value
                ------                          --------
Loop protect     Enabled                 Enabled
```

Viewing information about the peer-keepalive configuration

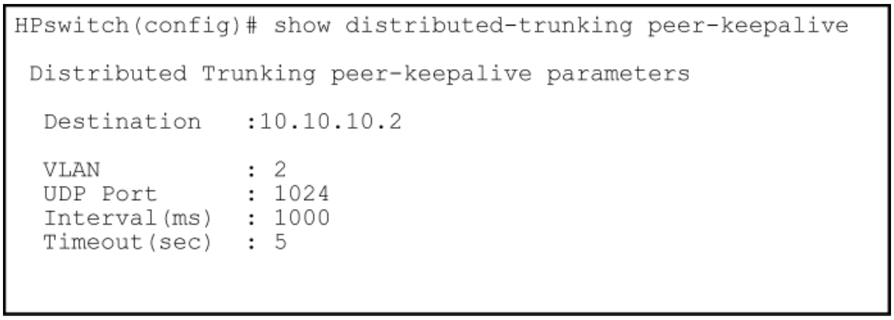
Syntax:

```
show distributed-trunking peer-keepalive
```

Displays information about peer-keepalive parameters.

Example

Figure 46 Output displaying peer-keepalive settings



```
HPswitch(config)# show distributed-trunking peer-keepalive

 Distributed Trunking peer-keepalive parameters

  Destination    :10.10.10.2

  VLAN           : 2
  UDP Port       : 1024
  Interval(ms)   : 1000
  Timeout(sec)   : 5
```

Viewing the switch interconnect information

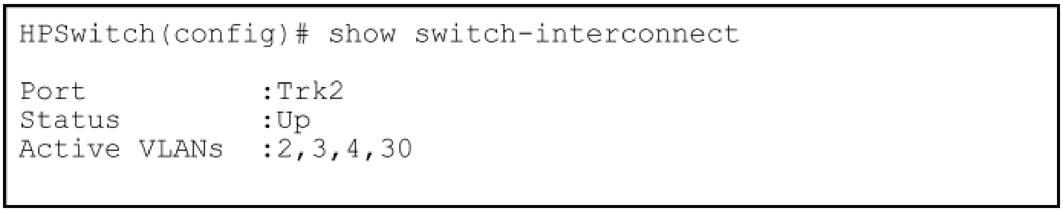
Syntax:

`show switch-interconnect`

Displays information about switch interconnect settings.

Example

Figure 47 Switch-interconnect settings

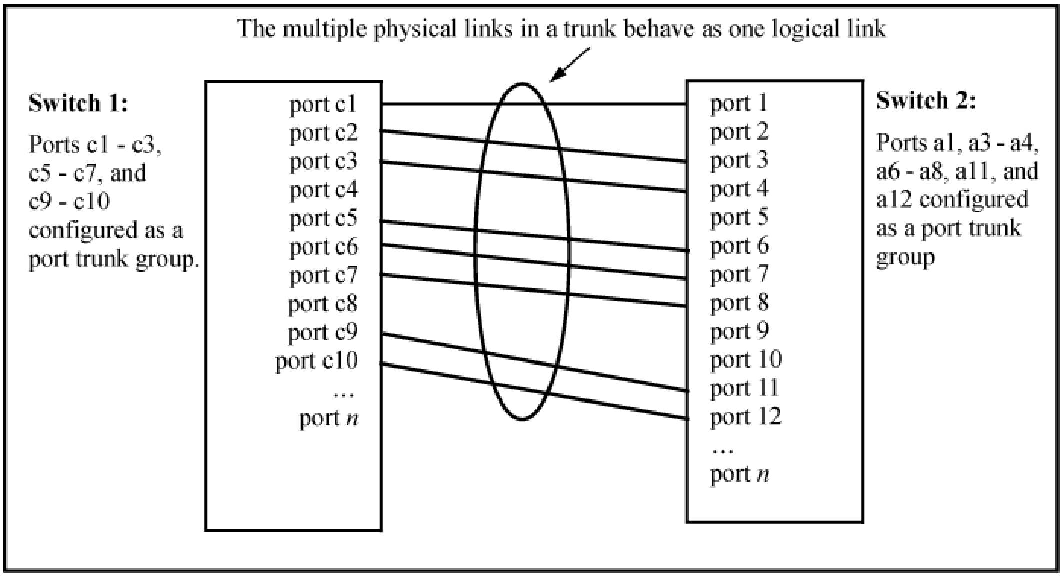


```
HPSwitch(config)# show switch-interconnect

Port            :Trk2
Status          :Up
Active VLANs    :2,3,4,30
```

Overview of port trunking

Port trunking allows you to assign up to eight physical links to one logical link (trunk) that functions as a single, higher-speed link providing dramatically increased bandwidth. This capability applies to connections between backbone devices as well as to connections in other network areas where traffic bottlenecks exist. A *trunk group* is a set of up to eight ports configured as members of the same port trunk. The ports in a trunk group do not have to be consecutive. For example:

Figure 48 Conceptual example of port trunking


The multiple physical links in a trunk behave as one logical link
Switch 1:
Ports c1 - c3, c5 - c7, and c9 - c10 configured as a port trunk group.
port c1
port c2
port c3
port c4
port c5
port c6
port c7
port c8
port c9
port c10
...
port *n*
port 1
port 2
port 3
port 4
port 5
port 6
port 7
port 8
port 9
port 10
port 11
port 12
...
port *n*
Switch 2:
Ports a1, a3 - a4, a6 - a8, a11, and a12 configured as a port trunk group

With full-duplex operation in a eight-port trunk group, trunking enables the following bandwidth capabilities:

Port connections and configuration

All port trunk links must be point-to-point connections between a switch and another switch, router, server, or workstation configured for port trunking. No intervening, non-trunking devices are allowed. It is important to note that ports on both ends of a port trunk group must have the same mode (speed and duplex) and flow control settings.

CAUTION: To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports you want to add to or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

NOTE:

Link connections

The switch does not support port trunking through an intermediate, non-trunking device such as a hub, or using more than onemedia type in a port trunk group. Similarly, for proper trunk operation, all links in the same trunk group must have the samespeed, duplex, and flow control.

Port security restriction

Port security does not operate on a trunk group. If you configure port security on one or more ports that are later added to a trunk group, the switch resets the port security parameters for those ports to the factory-default configuration.

Port trunk features and operation

The switches covered in this guide offer these options for port trunking:

- LACP: IEEE 802.3ad—Enabling L4-based trunk load balancing (CLI)
- Trunk: Non-Protocol—Trunk group operation using the "trunk" option

Up to 144 trunk groups are supported on the switches. The actual maximum depends on the number of ports available on the switch and the number of links in each trunk. (Using the link aggregation control protocol—LACP—option, you can include standby trunked ports in addition to the maximum of eight actively trunking ports.) The trunks do not have to be the same size; for example, 100 two-port trunks and 11 eight-port trunks are supported.

NOTE: LACP requires full-duplex (FDx) links of the same media type (10/100Base-T, 100FX, and so on) and the same speed, and enforces speed and duplex conformance across a trunk group. For most installations, HP Switch recommends that you leave the port Mode settings at `Auto` (the default). LACP also operates with `Auto-10`, `Auto-100`, and `Auto-1000 (if negotiation selects FDx)`, and `10FDx`, `100FDx`, and `1000FDx` settings. (The 10-gigabit ports available for some switch models allow only the `Auto` setting.)

Fault tolerance

If a link in a port trunk fails, the switch redistributes traffic originally destined for that link to the remaining links in the trunk. The trunk remains operable as long as there is at least one link in operation. If a link is restored, that link is automatically included in the traffic distribution again. The LACP option also offers a standby link capability, which enables you to keep links in reserve for service if one or more of the original active links fails. (See “Trunk group operation using LACP” (page 123).)

Trunk configuration methods

Dynamic LACP trunk

The switch automatically negotiates trunked links between LACP-configured ports on separate devices, and offers one dynamic trunk option: LACP. To configure the switch to initiate a dynamic LACP trunk with another device, use the `interface` command in the CLI to set the default LACP option to `active` on the ports you want to use for the trunk. For example, the following command sets ports C1 to C4 to `LACP active`:

```
HP Switch(config) int c1-c4 lacp active
```

The preceding example works if the ports are not already operating in a trunk. To change the LACP option on ports already operating as a trunk, you must first remove them from the trunk. For example, if ports C1 to C4 are LACP-active and operating in a trunk with another device, you would do the following to change them to LACP-passive:

```
HP Switch(config)# no int c1-c4 lacp
```

removes the ports from the trunk

```
HP Switch(config)# int c1-c4 lacp passive
```

configures LACP passive.

Dynamic LACP Standby Links

Dynamic LACP trunking enables you to configure standby links for a trunk by including more than eight ports in a dynamic LACP trunk configuration. When eight ports (trunk links) are up, the remaining link(s) will be held in standby status. If a trunked link that is “Up” fails, it will be replaced by a standby link, which maintains your intended bandwidth for the trunk. (Refer to also the “Standby” entry under “Port Status” in "Table 4-5. LACP Port Status Data" on page 4-22.) In the next example, ports A1 through A9 have been configured for the same LACP trunk. Notice that one of the links shows Standby status, while the remaining eight links are “Up”.

```
HP Switch> show lacp
                              LACP
       LACP      Trunk    Port                LACP    Admin    Oper
Port   Enabled   Group    Status   Partner   Status   Key      Key
----   -------   -----    ------   -------   ------   ----    -----
Al     Active     Dyn1     Up        Yes     Success   100      100
```

```
A2     Active     Dyn1     Up         Yes     Success   100      100
A3     Active     Dyn1     Up         Yes     Success   100      100
A4     Active     Dyn1     Up         Yes     Success   100      100
A5     Active     Dyn1     Up         Yes     Success   100      100
A6     Active     Dyn1     Up         Yes     Success   100      100
A7     Active     Dyn1     Up         Yes     Success   100      100
A8     Active     Dyn1     Up         Yes     Success   100      100
A9     Active     Dyn1    Standby     Yes     Success   100      100
```

Displaying LACP Local Information

```
HP Switch# show lacp local
LACP Local Information.
System ID: 001871-b98500
               LACP                Tx      Rx Timer
Port   Trunk   Mode   Aggregated   Timer   Expired
----- ------- ------- ----------- ------ ---------
A2       A2    Active    Yes       Fast    No
A3       A3    Active    Yes       Fast    No
```

Displaying LACP Peer Information

Use the `show lacp peer` command to display information about LACP peers. The System ID represents the MAC address of a partner switch. It will be zero if a partner is not found.

```
HP Switch(config)# show lacp peer
LACP Peer Information.
System ID: 001871-b98500
Local  Local                         Port       Oper    LACP    Tx
Port   Trunk   System ID      Port   Priority   Key     Mode    Timer
------ ------ --------------  ----- --------- ------- -------- -----
A2     A2      123456-654321   2       0       100    Passive   Fast
A3     A3      234567-456789   3       0       100    Passive   Fast
```

Displaying LACP Counters

Use the show lacp counters command to display statistical information about LACP ports.

Note on the Marker Protocol. Data traffic can be dynamically redistributed in port channels. This may occur when a link is added or removed, or there is a change in load-balancing. Traffic that is redistributed in the middle of a traffic flow could potentially cause mis-ordered data packets.

LACP uses the marker protocol to prevent data packets from being duplicated or reordered due to redistribution. Marker PDUs are sent on each port-channel link. The remote system responds to the marker PDU by sending a marker responder when it has received all the frames received on this link prior to the marker PDU. When the marker responders are received by the local system on all member links of the port channel, the local system can redistribute the packets in the traffic flow correctly.

For the switches covered in this guide, the marker BPDUs are not initiated, only forwarded when received, resulting in the Marker fields in the output usually displaying zeros.

```
HP Switch(config)# show lacp counters
LACP Port Counters.
               LACP      LACP      Marker    Marker    Marker     Marker
Port   Trunk   PDUs Tx   PDUs Rx   Req. Tx   Req. Rx   Resp. Tx   Resp. Rx   Error
----   ------  -------   -------   -------   -------   --------   --------   -----
A2       A2    1234      1234       0          0         0          0          0
A3       A3    1234      1234       0          0         0          0          0
```

Using keys to control dynamic LACP trunk configuration

The `lacp key` option provides the ability to control dynamic trunk configuration. Ports with the same key will be aggregated as a single trunk.

There are two types of keys associated with each port, the Admin key and the Operational key. The Operational key is the key currently in use. The Admin key is used internally to modify the value of the Operational key. The Admin and Operational key are usually the same, but using static LACP can alter the Operational key during runtime, in which case the keys would differ.

The `lacp key` command configures both the Admin and Operational keys when using dynamic LACP trunks. It only configures the Admin key if the trunk is a static LACP trunk. It is executed in the interface context.

Static trunk

The switch uses the links you configure with the Port/Trunk Settings screen in the menu interface or the `trunk` command in the CLI to create a static port trunk. The switch offers two types of static trunks: LACP and Trunk.

Table 13 Trunk types used in static and dynamic trunk groups

Trunking method	LACP	Trunk
Dynamic	Yes	No
Static	Yes	Yes

Table 14 describes the trunking options for LACP and Trunk protocols.

Table 14 Trunk configuration protocols

Protocol	Trunking Options
LACP (802.3ad)	Provides dynamic and static LACP trunking options. • **Dynamic LACP** — Use the switch-negotiated dynamic LACP trunk when: • The port on the other end of the trunk link is configured for Active or Passive LACP. • You want fault-tolerance for high-availability applications. If you use an eight-link trunk, you can also configure one or more additional links to operate as standby links that will activate only if another active link goes down. • **Static LACP** — Use the manually configured static LACP trunk when: • The port on the other end of the trunk link is configured for a static LACP trunk. • You want to configure non-default spanning tree or IGMP parameters on an LACP trunk group. • You want an LACP trunk group to operate in a VLAN other than the default VLAN and GVRP is disabled. (See “VLANs and dynamic LACP” (page 127).) • You want to use a monitor port on the switch to monitor an LACP trunk. For more information, see “Enabling L4-based trunk load balancing (CLI)” (page 108).
Trunk (non-protocol)	Provides manually configured, static-only trunking to: • Most HP Switch and routing switches not running the 802.3ad LACP protocol. • Windows NT and HP-UX workstations and servers

Table 14 Trunk configuration protocols *(continued)*

Protocol	Trunking Options
	Use the Trunk option when: • The device to which you want to create a trunk link is using a non-802.3ad trunking protocol. • You are unsure which type of trunk to use, or the device to which you want to create a trunk link is using an unknown trunking protocol. • You want to use a monitor port on the switch to monitor traffic on a trunk. See "Trunk group operation using the "trunk" option" (page 129).

General operating rules for port trunks

Media: For proper trunk operation, all ports on both ends of a trunk group must have the same media type and mode (speed and duplex). (For the switches, HP Switch recommends leaving the port Mode setting at `Auto` or, in networks using Cat 3 cabling, `Auto-10`.)

Port Configuration The default port configuration is `Auto`, which enables a port to sense speed and negotiate duplex with an auto-enabled port on another device. HP Switch recommends that you use the `Auto` setting for all ports you plan to use for trunking. Otherwise, you must manually ensure that the mode setting for each port in a trunk is compatible with the other ports in the trunk.

Figure 49 Recommended port mode setting for LACP

```
HP Switch(config)# show interfaces config

 Port Settings

  Port  Type      | Enabled Mode         Flow Ctrl MDI
  ----- --------- + ------- ------------ --------- ----
  1     10/100TX  | Yes     Auto         Enable    Auto
  2     10/100TX  | Yes     Auto         Enable    MDI
```

All of the following operate on a per-port basis, regardless of trunk membership:

- Enable/Disable
- Flow control (Flow Ctrl)

LACP is a full-duplex protocol. See "Enabling L4-based trunk load balancing (CLI)" (page 108).

Trunk configuration: All ports in the same trunk group must be the same trunk type (LACP or trunk). All LACP ports in the same trunk group must be either all static LACP or all dynamic LACP.

A trunk appears as a single port labeled`Dyn1`(for an LACP dynamic trunk) or `Trk1` (for a static trunk of type LACP, Trunk) on various menu and CLI screens. For a listing of which screens show which trunk types, see"How the switch lists trunk data" (page 129)

For spanning-tree or VLAN operation, configuration for all ports in a trunk is done at the trunk level. (You cannot separately configure individual ports within a trunk for spanning-tree or VLAN operation.)

Traffic distribution:

All of the switch trunk protocols use the SA/DA (source address/destination address) method of distributing traffic across the trunked links. See "Outbound traffic distribution across trunked links" (page 129).

Spanning Tree:

802.1D (STP) and 802.1w (RSTP) Spanning Tree operate as a global setting on the switch (with one instance of Spanning Tree per switch). 802.1s (MSTP) Spanning Tree operates on a per-instance basis (with multiple instances allowed per switch). For each Spanning Tree instance, you can adjust Spanning Tree parameters on a per-port basis.

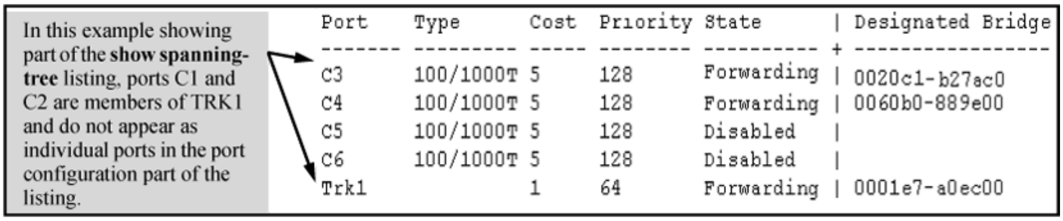
A static trunk of any type appears in the Spanning Tree configuration display, and you can configure Spanning Tree parameters for a static trunk in the same way that you would configure Spanning Tree parameters on a non-trunked port. (Note that the switch lists the trunk by name—such as Trk1—and does not list the individual ports in the trunk.) For example, if ports C1 and C2 are configured as a static trunk named Trk1, they are listed in the Spanning Tree display as Trk1 and do not appear as individual ports in the Spanning Tree displays. See Figure 50 (page 119).

When Spanning Tree forwards on a trunk, all ports in the trunk will be forwarding. Conversely, when Spanning Tree blocks a trunk, all ports in the trunk are blocked.

NOTE: A dynamic LACP trunk operates only with the default Spanning Tree settings. Also, this type of trunk appears in the CLI **show spanning-tree** display, but not in the Spanning Tree Operation display of the Menu interface.

If you remove a port from a static trunk, the port retains the same Spanning Tree settings that were configured for the trunk.

Figure 50 Example of a port trunk in a Spanning Tree listing



In this example showing part of the **show spanning-tree** listing, ports C1 and C2 are members of TRK1 and do not appear as individual ports in the port configuration part of the listing.

```
Port    Type       Cost  Priority State      | Designated Bridge
------- ---------- ----- -------- ---------- + ------------------
C3      100/1000T  5     128      Forwarding | 0020c1-b27ac0
C4      100/1000T  5     128      Forwarding | 0060b0-889e00
C5      100/1000T  5     128      Disabled   |
C6      100/1000T  5     128      Disabled   |
Trk1               1     64       Forwarding | 0001e7-a0ec00
```

IP multicast protocol (IGMP):

A static trunk of any type appears in the IGMP configuration display, and you can configure IGMP for a static trunk in the same way that you would configure IGMP on a non-trunked port. (Note that the switch lists the trunk by name—such as Trk1—and does not list the individual ports in the trunk.) Also, creating a new trunk automatically places the trunk in IGMP Auto status if IGMP is enabled for the default VLAN.

A dynamic LACP trunk operates only with the default IGMP settings and does not appear in the IGMP configuration display or `show ip igmp` listing.

VLANs:

Creating a new trunk automatically places the trunk in the DEFAULT_VLAN, regardless of whether the ports in the trunk were in another VLAN. Similarly, removing a port from a trunk group automatically places the port in the default VLAN. You can configure a static trunk in the same way that you configure a port for membership in any VLAN.

NOTE: For a dynamic LACP trunk to operate in a VLAN other than the default VLAN (DEFAULT_VLAN), GVRP must be enabled. See “Enabling L4-based trunk load balancing (CLI)” (page 108).

Port security:

Trunk groups (and their individual ports) cannot be configured for port security, and the switch excludes trunked ports from the `show port-security` listing. If you configure non-default port security settings for a port, then subsequently try to place the port in a trunk, you see the following message and the command is not executed:

`port-list` Command cannot operate over a logical port.

Monitor port:

NOTE: A trunk cannot be a monitor port. A monitor port can monitor a static trunk but cannot monitor a dynamic LACP trunk.

About configuring a static or dynamic trunk group

IMPORTANT: Configure port trunking *before* you connect the trunked links between switches. Otherwise, a broadcast storm could occur. (If you need to connect the ports before configuring them for trunking, you can temporarily disable the ports until the trunk is configured. See "Enabling or Disabling Ports and Configuring Port Mode".)

The table on Table 13 describes the maximum number of trunk groups you can configure on the switch. An individual trunk can have up to eight links, with additional standby links if you are using LACP. You can configure trunk group types as follows:

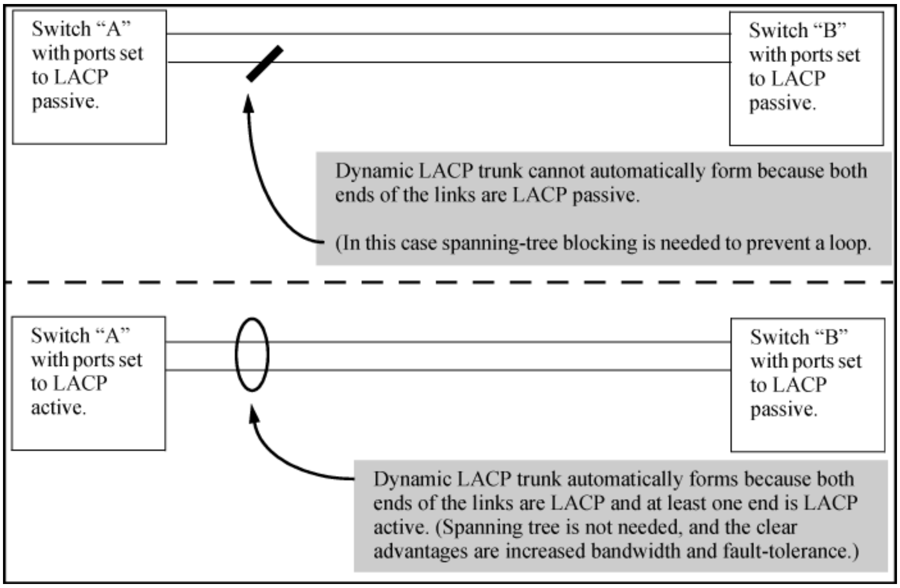
Trunk Type	**Trunk Group Membership**	
	TrkX (static)	**DynX (dynamic)**
LACP	Yes	Yes
Trunk	Yes	No

About enabling a dynamic LACP trunk group

In the default port configuration, all ports on the switch are set to disabled. To enable the switch to automatically form a trunk group that is dynamic on both ends of the link, the ports on one end of a set of links must be LACP Active. The ports on the other end can be either LACP Activeor LACP Passive. The `active` command enables the switch to automatically establish a (dynamic) LACP trunk group when the device on the other end of the link is configured for LACP Passive.

Example

Figure 51 Criteria for automatically forming a dynamic LACP trunk


Switch "A" with ports set to LACP passive.
Switch "B" with ports set to LACP passive.
Dynamic LACP trunk cannot automatically form because both ends of the links are LACP passive.
(In this case spanning-tree blocking is needed to prevent a loop.
Switch "A" with ports set to LACP active.
Switch "B" with ports set to LACP passive.
Dynamic LACP trunk automatically forms because both ends of the links are LACP and at least one end is LACP active. (Spanning tree is not needed, and the clear advantages are increased bandwidth and fault-tolerance.)

Dynamic LACP standby links

Dynamic LACP trunking enables you to configure standby links for a trunk by including more than eight ports in a dynamic LACP trunk configuration. When eight ports (trunk links) are up, the remaining links are held in standby status. If a trunked link that is "Up" fails, it is replaced by a standby link, which maintains your intended bandwidth for the trunk. (See also the "Standby" entry under "Port Status" in Table 16.) In the next example, ports A1 through A9 have been configured for the same LACP trunk. Notice that one of the links shows `Standby` port status, while the remaining eight links show `Up` port status.

Example

Example 38 A dynamic LACP trunk with one standby link

```
HP Switch> show lacp

                              LACP

      LACP      Trunk     Port                LACP      Admin  Oper
Port  Enabled   Group     Status    Partner   Status    Key    Key
----  -------   -------   -------   -------   -------   ------ ------
Al    Active    Dyn1      Up        Yes       Success   100    100
A2    Active    Dyn1      Up        Yes       Success   100    100
A3    Active    Dyn1      Up        Yes       Success   100    100
A4    Active    Dyn1      Up        Yes       Success   100    100
A5    Active    Dyn1      Up        Yes       Success   100    100
A6    Active    Dyn1      Up        Yes       Success   100    100
A7    Active    Dyn1      Up        Yes       Success   100    100
A8    Active    Dyn1      Up        Yes       Success   100    100
A9    Active    Dyn1      Standby   Yes       Success   100    100
```

Displaying LACP local information

Example 39 Example of LACP local information

```
HP Switch# show lacp local

LACP Local Information.

System ID: 001871-b98500

              LACP                  Tx     Rx Timer
  Port Trunk  Mode      Aggregated  Timer  Expired
  ---- ------ --------  ----------- ------ --------
  A2   A2     Active    Yes         Fast   No
  A3   A3     Active    Yes         Fast   No
```

Displaying LACP peer information

Use the `show lacp peer` command to display information about LACP peers. The System ID represents the MAC address of a partner switch. It will be zero if a partner is not found.

Example 40 Example of LACP peer information

```
HP Switch(config)# show lacp peer

LACP Peer Information.

System ID: 001871-b98500

  Local  Local                          Port       Oper     LACP      Tx
  Port   Trunk  System ID        Port  Priority   Key      Mode      Timer
  ------ ------ -------------- ----- --------- ------- -------- -----
  A2     A2     123456-654321  2     0          100      Passive   Fast
  A3     A3     234567-456789  3     0          100      Passive   Fast
```

Displaying LACP counters

Use the `show lacp counters` command to display statistical information about LACP ports.

Note on the Marker Protocol. Data traffic can be dynamically redistributed in port channels. This may occur when a link is added or removed, or there is a change in load-balancing. Traffic that is redistributed in the middle of a traffic flow could potentially cause mis-ordered data packets.

LACP uses the marker protocol to prevent data packets from being duplicated or reordered due to redistribution. Marker PDUs are sent on each port-channel link. The remote system responds to the marker PDU by sending a marker responder when it has received all the frames received on this link prior to the marker PDU. When the marker responders are received by the local system on all member links of the port channel, the local system can redistribute the packets in the traffic flow correctly.

For the switches covered in this guide, the marker BPDUs are not initiated, only forwarded when received, resulting in the Marker fields in the output usually displaying zeros.

Example 41 Example of LACP counters output

```
HP Switch(config)# show lacp counters

LACP Port Counters.


  LACP        LACP      Marker    Marker   Marker   Marker
  Port Trunk  PDUs Tx   PDUs Rx   Req. Tx  Req. Rx  Resp. Tx Resp. Rx Error
  ---- ------ --------- --------- -------- -------- -------- -------- --------
  A2   A2     1234      1234      0        0        0        0        0
  A3   A3     1234      1234      0        0        0        0        0
```

Trunk group operation using LACP

The switch can automatically configure a dynamic LACP trunk group, or you can manually configure a static LACP trunk group.

NOTE: LACP requires full-duplex (FDx) links of the same media type (10/100Base-T, 100FX, and so on) and the same speed and enforces speed and duplex conformance across a trunk group. For most installations, HP Switch recommends that you leave the port mode settings at `Auto` (the default). LACP also operates with `Auto-10`, `Auto-100`, and `Auto-1000` (if negotiation selects FDx), and `10FDx`, `100FDx`, and `1000FDx` settings.

LACP trunk status commands include:

Trunk display method	Static LACP trunk	Dynamic LACP trunk
CLI `show lacp` command	Included in listing.	Included in listing.
CLI `show trunk` command	Included in listing.	Not included.
Port/Trunk Settings screen in menu interface	Included in listing.	Not included

Thus, to display a listing of dynamic LACP trunk ports, you must use the `show lacp` command.

In most cases, trunks configured for LACP on the switches operate as described in Table 15 (page 123).

Table 15 LACP trunk types

LACP port trunk configuration	Operation
Dynamic LACP	This option automatically establishes an 802.3ad-compliant trunk group, with **LACP** for the port Type parameter and **DynX** for the port Group name, where **X** is an automatically assigned value from 1 to 144, depending on how many dynamic and static trunks are currently on the switch. (The switch allows a maximum of 144 trunk groups in any combination of static and dynamic trunks.)

Table 15 LACP trunk types *(continued)*

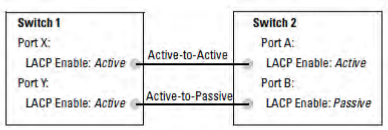
LACP port trunk configuration	Operation
	NOTE: Dynamic LACP trunks operate only in the default VLAN (unless GVRP is enabled and `Forbid` is used to prevent the trunked ports from joining the default VLAN). Thus, if an LACP dynamic port forms using ports that are not in the default VLAN, the trunk automatically moves to the default VLAN unless GVRP operation is configured to prevent this from occurring. In some cases, this can create a traffic loop in your network. For more information on this topic, see"VLANs and dynamic LACP" (page 127). Under the following conditions, the switch automatically establishes a dynamic LACP port trunk group and assigns a port Group name: • The ports on both ends of each link have compatible mode settings (speed and duplex). • The port on one end of each link must be configured for LACP Active and the port on the other end of the same link must be configured for either LACP Passive or LACP Active. For example:  Switch 1 Port X: LACP Enable: *Active* Port Y: LACP Enable: *Active* Active-to-Active Active-to-Passive Switch 2 Port A: LACP Enable: *Active* Port B: LACP Enable: *Passive* Either of the above link configurations allows a dynamic LACP trunk link. **Backup Links:** A maximum of eight operating links are allowed in the trunk, but, with dynamic LACP, you can configure one or more additional (backup) links that the switch automatically activates if a primary link fails. To configure a link as a standby for an existing eight-port dynamic LACP trunk, ensure that the ports in the standby link are configured as either active-to-active or active-to-passive between switches. **Displaying dynamic LACP trunk data:** To list the configuration and status for a dynamic LACP trunk, use the CLI `show lacp` command. **NOTE:** The dynamic trunk is automatically created by the switch and is not listed in the static trunk listings available in the menu interface or in the CLI `show trunk` listing.
Static LACP	Provides a manually configured, static LACP trunk to accommodate these conditions: • The port on the other end of the trunk link is configured for a static LACP trunk. • You want to configure non-default Spanning Tree or IGMP parameters on an LACP trunk group. • You want an LACP trunk group to operate in a VLAN other than the default VLAN and GVRP is disabled. (See "VLANs and dynamic LACP" (page 127).) • You want to use a monitor port on the switch to monitor an LACP trunk.

Table 15 LACP trunk types *(continued)*

LACP port trunk configuration	Operation
	The trunk operates if the trunk group on the opposite device is running one of the following trunking protocols: • Active LACP • Passive LACP • Trunk This option uses **LACP** for the port Type parameter and **TrkX** for the port Group parameter, where **X** is an automatically assigned value in a range corresponding to the maximum number of trunks the switch allows. (The table on Table 13 (page 117) lists the maximum number of trunk groups allowed on the switches.) **Displaying static LACP trunk data :** To list the configuration and status for a static LACP trunk, use the CLI `show lacp` command. To list a static LACP trunk with its assigned ports, use the CLI `show trunk` command or display the menu interface Port/Trunk Settings screen. Static LACP does not allow standby ports.

Default port operation

In the default configuration, LACP is disabled for all ports. If LACP is not configured as Active on at least one end of a link, the port does not try to detect a trunk configuration and operates as a standard, untrunked port. Table 16 (page 125) lists the elements of per-port LACP operation. To display this data for a switch, execute the following command in the CLI:

```
HP Switch show lacp
```

Table 16 LACP port status data

Status name	Meaning
Port Numb	Shows the physical port number for each port configured for LACP operation (C1, C2, C3 …). Unlisted port numbers indicate that the missing ports that are assigned to a static trunk group are not configured for any trunking.
LACP Enabled	**Active:** The port automatically sends LACP protocol packets. **Passive:** The port does not automatically send LACP protocol packets and responds only if it receives LACP protocol packets from the opposite device. A link having either two active LACP ports or one active port and one passive port can perform dynamic LACP trunking. A link having two passive LACP ports does not perform LACP trunking because both ports are waiting for an LACP protocol packet from the opposite device. **NOTE:** In the default switch configuration, LACP is disabled for all ports.
Trunk Group	**TrkX:** This port has been manually configured into a static LACP trunk. **Trunk group same as port number:** The port is configured for LACP, but is not a member of a port trunk.
Port Status	**Up:** The port has an active LACP link and is not blocked or in standby mode. **Down:** The port is enabled, but an LACP link is not established. This can indicate, for example, a port that is

Table 16 LACP port status data *(continued)*

Status name	Meaning
	not connected to the network or a speed mismatch between a pair of linked ports. **Disabled:** The port cannot carry traffic. **Blocked:** LACP, Spanning Tree has blocked the port. (The port is not in LACP standby mode.) This may be caused by a (brief) trunk negotiation or a configuration error, such as differing port speeds on the same link or trying to connect the switch to more trunks than it can support. (See the table on Table 14.) **NOTE:** Some older devices are limited to four ports in a trunk. When eight LACP-enabled ports are connected to one of these older devices, four ports connect, but the other four ports are blocked. **Standby:** The port is configured for dynamic LACP trunking to another device, but the maximum number of ports for the dynamic trunk to that device has already been reached on either the switch or the other device. This port will remain in reserve, or "standby" unless LACP detects that another, active link in the trunk has become disabled, blocked, or down. In this case, LACP automatically assigns a standby port, if available, to replace the failed port.
LACP Partner	**Yes:** LACP is enabled on both ends of the link. **No:** LACP is enabled on the switch, but either LACP is not enabled or the link has not been detected on the opposite device.
LACP Status	**Success:** LACP is enabled on the port, detects and synchronizes with a device on the other end of the link, and can move traffic across the link. **Failure:** LACP is enabled on a port and detects a device on the other end of the link, but is not able to synchronize with this device, and therefore is not able to send LACP packets across the link. This can be caused, for example, by an intervening device on the link (such as a hub), a bad hardware connection, or if the LACP operation on the opposite device does not comply with the IEEE 802.3ad standard.

LACP notes and restrictions

802.1X (Port-based access control) configured on a port

To maintain security, LACP is not allowed on ports configured for 802.1X authenticator operation. If you configure port security on a port on which LACP (active or passive) is configured, the switch removes the LACP configuration, displays a notice that LACP is disabled on the port, and enables 802.1X on that port.

```
HP Switch(config)# aaa port-access authenticator b1
LACP has been disabled on 802.1x port(s).
HP Switch(config)#
```

The switch does not allow you to configure LACP on a port on which port access (802.1X) is enabled. For example:

```
HP Switch(config)# int b1 lacp passive
Error configuring port  port-number  : LACP and 802.1x cannot
```

```
be run together.
HP Switch(config)#
```

To restore LACP to the port, you must first remove the 802.1X configuration of the port and then re-enable LACP active or passive on the port.

Port securityconfigured on a port

To maintain security, LACP is not allowed on ports configured for port security. If you configure port security on a port on which LACP (active or passive) is configured, the switch removes the LACP configuration, displays a notice that LACP is disabled on the port, and enables port security on that port. For example:

```
HP Switch(config)# port-security a17 learn-mode static address-
limit 2 LACP has been disabled on secured port(s).
HP Switch(config)#
```

The switch does not allow you to configure LACP on a port on which port security is enabled. For example:

```
HP Switch(config)# int a17 lacp passive
Error configuring port A17: LACP and port security cannot be
run together.
HP Switch(config)#
```

To restore LACP to the port, you must remove port security and re-enable LACP active or passive.

Changing trunking methods

To convert a trunk from static to dynamic, you must first eliminate the static trunk.

Static LACP trunks

When a port is configured for LACP (active or passive), but does not belong to an existing trunk group, you can add that port to a static trunk. Doing so disables dynamic LACP on that port, which means you must manually configure both ends of the trunk.

Dynamic LACP trunks

You can configure a port for LACP-active or LACP-passive, but on a dynamic LACP trunk you cannot configure the other options that you can on static trunks. If you want to manually configure a trunk, use the `trunk` command. (See "Using the CLI To Configure a Static or Dynamic Trunk Group")

VLANs and dynamic LACP

A dynamic LACP trunk operates only in the default VLAN (unless you have enabled GVRP on the switch and use `Forbid` to prevent the ports from joining the default VLAN).

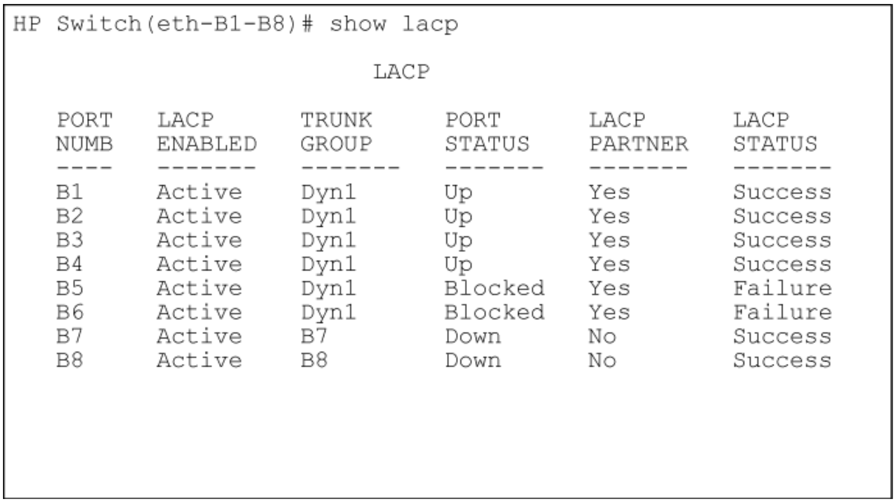
If you want to use LACP for a trunk on a non-default VLAN and GVRP is disabled, configure the trunk as a static trunk.

Blocked ports with older devices.

Some older devices are limited to four ports in a trunk. When eight LACP-enabled ports are connected to one of these older devices, four ports connect, but the other four ports are blocked. The LACP status of the blocked ports is shown as "Failure."

If one of the other ports becomes disabled, a blocked port replaces it (Port Status becomes "Up"). When the other port becomes active again, the replacement port goes back to blocked (Port Status is "Blocked"). It can take a few seconds for the switch to discover the current status of the ports.

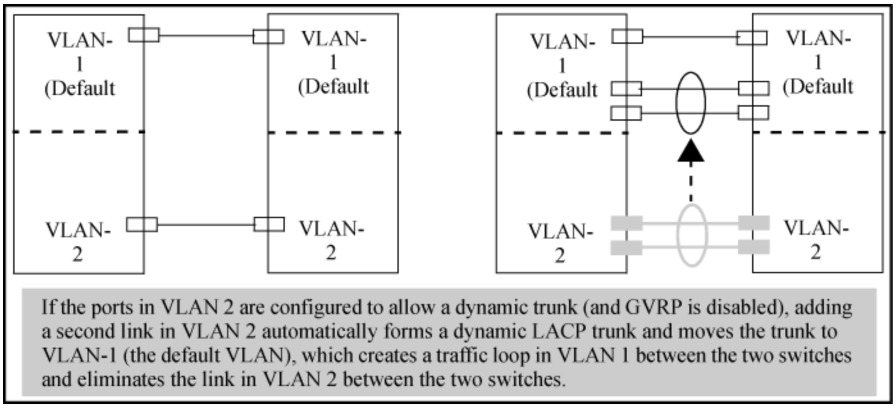
Figure 52 Blocked ports with LACP



```
HP Switch(eth-B1-B8)# show lacp

                         LACP

   PORT     LACP       TRUNK      PORT       LACP       LACP
   NUMB     ENABLED    GROUP      STATUS     PARTNER    STATUS
   ----     -------    -------    -------    -------    -------
   B1       Active     Dyn1       Up         Yes        Success
   B2       Active     Dyn1       Up         Yes        Success
   B3       Active     Dyn1       Up         Yes        Success
   B4       Active     Dyn1       Up         Yes        Success
   B5       Active     Dyn1       Blocked    Yes        Failure
   B6       Active     Dyn1       Blocked    Yes        Failure
   B7       Active     B7         Down       No         Success
   B8       Active     B8         Down       No         Success
```

If there are ports that you do not want on the default VLAN, ensure that they cannot become dynamic LACP trunk members. Otherwise a traffic loop can unexpectedly occur. For example:

Figure 53 A dynamic LACP trunk forming in a VLAN can cause a traffic loop



If the ports in VLAN 2 are configured to allow a dynamic trunk (and GVRP is disabled), adding a second link in VLAN 2 automatically forms a dynamic LACP trunk and moves the trunk to VLAN-1 (the default VLAN), which creates a traffic loop in VLAN 1 between the two switches and eliminates the link in VLAN 2 between the two switches.

Easy control methods include either disabling LACP on the selected ports or configuring them to operate in static LACP trunks.

Spanning Tree and IGMP

If Spanning Tree, IGMP, or both are enabled in the switch, a dynamic LACP trunk operates only with the default settings for these features and does not appear in the port listings for these features.

Half-duplex, different port speeds, or both not allowed in LACP trunks

Theports on both sides of an LACP trunk must be configured for the same speed and for full-duplex (FDx). The 802.3ad LACP standard specifies a full-duplex (FDx) requirement for LACP trunking. (10-gigabit ports operate only at FDx.)

A port configured as LACP passive and not assigned to a port trunk can be configured to half-duplex (HDx). However, in any of the following cases, a port cannot be reconfigured to an HDx setting:

- If the port is a 10-gigabit port.
- If a port is set to LACP Active, you cannot configure it to HDx.
- If a port is already a member of a static or dynamic LACP trunk, you cannot configure it to HDx.
- If a port is already set to HDx, the switch does not allow you to configure it for a static or dynamic LACP trunk.

Dynamic/static LACP interoperation

A port configured for dynamic LACP can properly interoperate with a port configured for static (TrkX) LACP, but any ports configured as standby LACP links are ignored.

Trunk group operation using the "trunk" option

Thismethod creates a trunk group that operates independently of specific trunking protocols and does not use a protocol exchange with the device on the other end of the trunk. With this choice, the switch simply uses the SA/DA method of distributing outbound traffic across the trunked ports without regard for how that traffic is handled by the device at the other end of the trunked links. Similarly, the switch handles incoming traffic from the trunked links as if it were from a trunked source.

When a trunk group is configured with the `trunk` option, the switch automatically sets the trunk to a priority of "4" for Spanning Tree operation (even if Spanning Tree is currently disabled). This appears in the running-config file as `spanning-tree Trkn priority 4`. Executing `write memory` after configuring the trunk places the same entry in the startup-config file.

Use the `trunk` option to establish a trunk group between a switch and another device, where the other device's trunking operation fails to operate properly with LACP trunking configured on the switches.

How the switch lists trunk data

Static trunk group	Appears in the menu interface and the output from the CLI `show trunk` and `show interfaces` commands.
Dynamic LACP trunk group	Appears in the output from the CLI `show lacp` command.

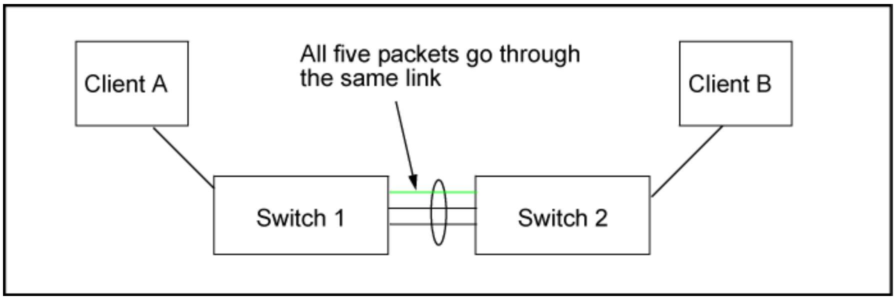
Interface option	**Dynamic LACP trunk group**	**Static LACP trunk group**	**Static non-protocol**
Menu interface	No	Yes	Yes
CLI `show trunk`	No	Yes	Yes
CLI `show interfaces`	No	Yes	Yes
CLI `show lacp`	Yes	Yes	No
CLI `show spanning-tree`	No	Yes	Yes
CLI `show igmp`	No	Yes	Yes
CLI `show config`	No	Yes	Yes

Outbound traffic distribution across trunked links

The two trunk group options (LACP and trunk) use SA/DA pairs for distributing outbound traffic over trunked links. That is, the switch sends traffic from the same source address to the same destination address through the same trunked link, and may also send traffic from the same source address to a different destination address through the same link or a different link, depending on the mapping of path assignments among the links in the trunk. Likewise, the switch distributes traffic for the same destination address but from different source addresses through links depending on the path assignment.

The load-balancing is done on a per-communication basis. Otherwise, traffic is transmitted across the same path as shown in Figure 54 (page 130). That is, if Client A attached to Switch 1 sends five packets of data to Server A attached to Switch 2, the same link is used to send all five packets. The SA/DA address pair for the traffic is the same. The packets are not evenly distributed across any other existing links between the two switches; they all take the same path.

Figure 54 Example of single path traffic through a trunk



The actual distribution of the traffic through a trunk depends on a calculation using bits from the SA/DA. When an IP address is available, the calculation includes the last five bits of the IP source address and IP destination address; otherwise, the MAC addresses are used. The result of that process undergoes a mapping that determines which link the traffic goes through. If you have only two ports in a trunk, it is possible that all the traffic will be sent through one port even if the SA/DA pairs are different. The more ports you have in the trunk, the more likely it is that the traffic will be distributed among the links.

When a new port is added to the trunk, the switch begins sending traffic, either new traffic or existing traffic, through the new link. As links are added or deleted, the switch redistributes traffic across the trunk group. For example, in Figure 55 (page 130) showing a three-port trunk, traffic could be assigned as shown in Table 17 (page 130).

Figure 55 Example of port-trunked network

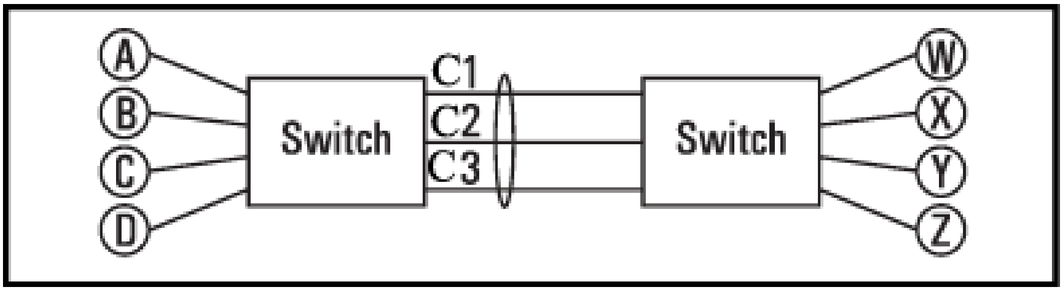


Table 17 Example of link assignments in a trunk group (SA/DA distribution)

Source	Destination	Link
Node A	Node W	1
Node B	Node X	2
Node C	Node Y	3
Node D	Node Z	1
Node A	Node Y	2
Node B	Node W	3

Because the amount of traffic coming from or going to various nodes in a network can vary widely, it is possible for one link in a trunk group to be fully utilized while other links in the same trunk have unused bandwidth capacity, even if the assignments were evenly distributed across the links in a trunk.

Trunk load balancing using Layer 4 ports

Trunk load balancing using Layer 4 ports allows the use of TCP/UDP source and destination port number for trunk load balancing. This is in addition to the current use of source and destination IP address and MAC addresses. Configuration of Layer 4 load balancing would apply to all trunks on the switch. Only non-fragmented packets will have their TCP/UDP port number used by load balancing. This ensures that all frames associated with a fragmented IP packet are sent through the same trunk on the same physical link.

The priority for using Layer 4 packets when this feature is enabled is as follows:

1. If the packet protocol is an IP packet and has Layer 4 port information, use Layer 4.
2. If the packet protocol is an IP packet and does *not* have Layer 4 information, use Layer 3 information.
3. If the packet is *not* an IP packet, use Layer 2 information.

Distributed trunking overview

The IEEE standard 802.3ad requires that all links in a trunk group originate from the same switch. Distributed trunking uses a proprietary protocol that allows two or more port trunk links distributed across two switches to create a trunk group. The grouped links appear to the downstream device as if they are from a single device. This allows third party devices such as switches, servers, or any other networking device that supports trunking to interoperate with the distributed trunking switches (DTSs) seamlessly. Distributed trunking provides device-level redundancy in addition to link failure protection.

DTSs are connected by a special interface called the InterSwitch-Connect (ISC) port. This interface exchanges information so that the DTSs appear as a single switch to a downstream device, as mentioned above. Each distributed trunk (DT) switch in a DT pair must be configured with a separate ISC link and peer-keepalive link. The peer-keepalive link is used to transmit keepalive messages when the ISC link is down to determine if the failure is a link-level failure or the complete failure of the remote peer.

The downstream device is a distributed trunking device (DTD). The DTD forms a trunk with the DTSs. The connecting links are DT links and the ports are DT ports. A distributed trunk can span a maximum of two switches.

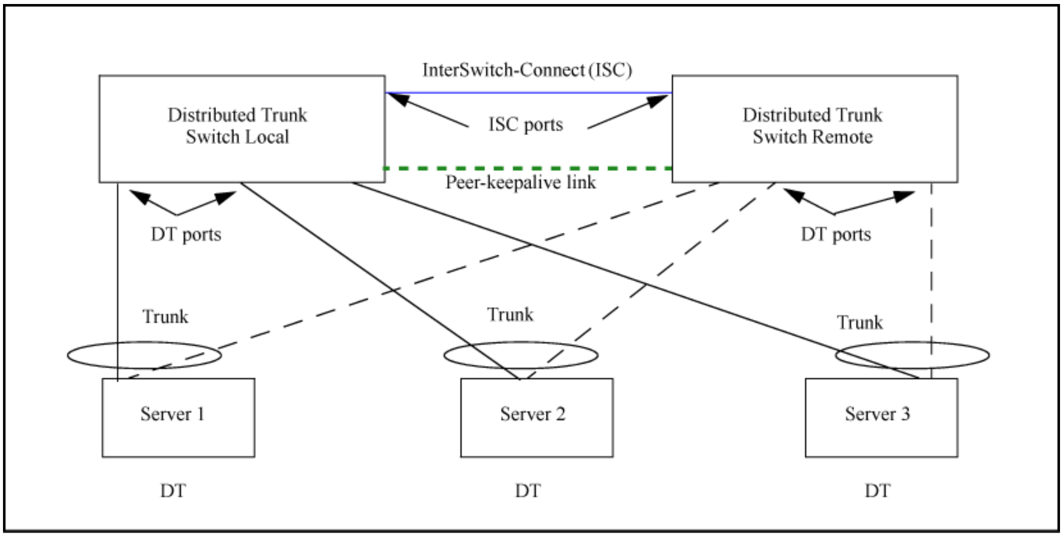
NOTE: All DT linked switches must be running the same software version.

You can group together distributed trunks by configuring two individual dt-lacp/dt-trunk trunks with the same trunk group name in each switch. The DT ports are grouped dynamically after the configuration of distributed trunking.

NOTE: Before you configure the switch, HP recommends that you review the “Distributed trunking restrictions” (page 139) for a complete list of operating notes and restrictions.

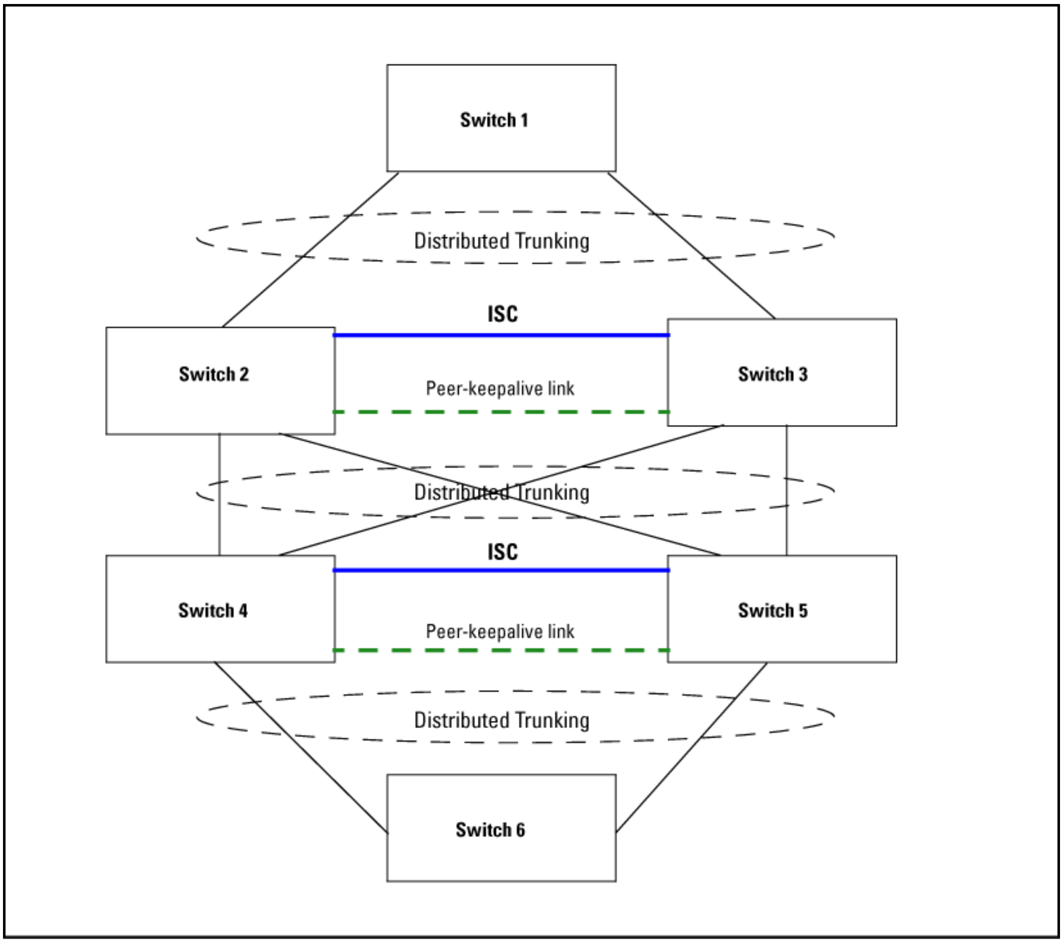
In Figure 56 (page 132), three different distributed trunks with three different servers have one common ISC link. Each trunk spans only two DTSs, which are connected at the ISC ports so they can exchange information that allows them to appear as one device to the server.

Figure 56 Example of distributed trunking with three different distributed trunks with three servers



An example of distributed trunking switch-to-switch in a square topology is shown in Figure 57 (page 132).

Figure 57 Example of a distributed trunking switch-to-switch square topology



Distributed trunking interconnect protocol

Distributed trunking uses the distributed trunking interconnect protocol (DTIP) to transfer DT-specific configuration information for the comparison process and to synchronize MAC and DHCP snooping binding data between the two DT peer switches.

NOTE: For DHCP snooping to function correctly in a DT topology, the system time must be the same on both switches, and the ISC must be trusted for DHCP snooping.

About configuring distributed trunking

The following parameters must be configured identically on the peer devices or undesirable behavior in traffic flow may occur:

- The ISC link must have a VLAN interface configured for the same VLAN on both DT switches.
- VLAN membership for all DT trunk ports should be the same on both DT switches in a DT pair.
- IGMP-snooping or DHCP-snooping configuration on a DT VLAN should be the same on both DT switches. For example, for a DT, if IGMP-snooping or DHCP-snooping is enabled on a VLAN that has a DT port as a member port of the VLAN, the same must be configured on the peer DT on the same VLAN.
- Loop-protection configuration on a DT VLAN should be the same for both DT switches.

About configuring peer-keepalive links

Distributed trunking uses UDP-based peer-keepalive messages to determine if an ISC link failure is at the link level or the peer has completely failed. The following operating rules must be followed to use peer-keepalive links:

- An IP address must be configured for a peer-keepalive VLAN interface and the same IP address must be configured as a peer-keepalive destination on the peer DT switch.
- There must be logical Layer 3 connectivity between the two IP addresses configured for the peer-keepalive VLAN interface.
- Only peer-keepalive messages are sent over the peer-keepalive VLAN (Layer 3 link). These messages indicate that the DT switch from which the message originates is up and running. No data or synchronization traffic is sent over the peer-keepalive VLAN.
- STP cannot run on peer-keepalive links.
- The peer-keepalive VLAN can have only one member port. If you attempt to assign a second member port to this VLAN, or if you attempt to configure a VLAN that has more than one member port as a peer-keepalive VLAN, this message displays:

  ```
  A keepalive VLAN can only have one member port.
  ```
- A port cannot be a member of a regular VLAN and a peer-keepalive VLAN. An error message displays:

  ```
  A port cannot simultaneously be a member of a keepalive and a
  non-keepalive VLAN.
  ```
- The DEFAULT VLAN cannot be a peer-keepalive VLAN. An error message displays:

  ```
  The default VLAN cannot be configured as a keepalive VLAN.
  ```

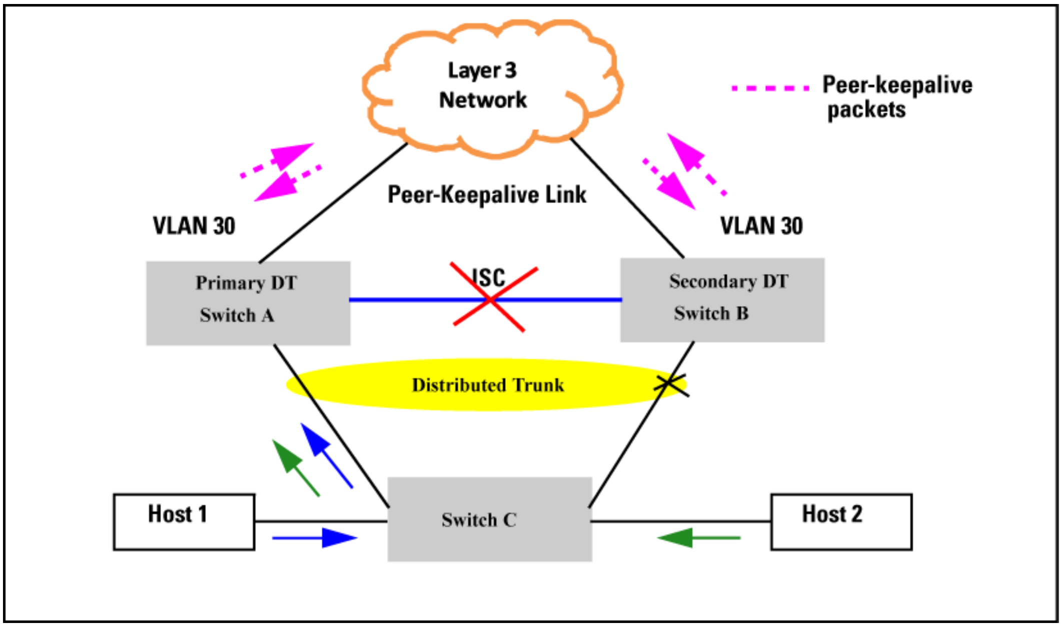
NOTE: If you are upgrading your software from a version prior to K.15.05.*xxxxx* with a configuration that violates any of the above operating rules, the following message displays:

```
DT: Keepalive mis-configuration detected. Reconfigure the keepalive
VLAN.
```

You must then manually correct the configuration.

DT switches have an operational role that depends on the system MAC address. The bridge with the lowest system MAC address acts as the DT primary device; the other device is the DT secondary device. These roles are used to determine which device forwards traffic when the ISC link is down.

Figure 58 Example of ISC link failure with peer-keepalive



Peer-keepalive messages are sent by both the DT switches as soon as the switches detect that the ISC link is down. Peer-keepalive message transmission (sending and receiving) is suspended until the peer-keepalive hold timer expires. When the hold timer expires, the DT switches begin sending peer-keepalive messages periodically while receiving peer-keepalive messages from the peer switch. If the DT switch fails to receive any peer-keepalive messages for the timeout period, it continues to forward traffic, assuming that the DT peer switch has completely failed.

Conversely, if the failure is because the ISC link went down and the secondary DT switch receives even one peer-keepalive message from the primary peer, the secondary switch disables all its DT ports. The primary switch always forwards the traffic on its DT ports even if it receives peer-keepalive messages from the secondary DT switch.

In both situations, if the ISC link or the DT switch becomes operational, both the DT peers sync the MAC addresses learned during the failover and continue to forward traffic normally. The peer-keepalive timers and operation is halted.

Maximum DT trunks and links supported

Table 18 (page 134) shows the maximum number of DT trunks and DT links that are supported.

Table 18 Maximum supported DT trunks and links

Description	Max number
Maximum number of groups (DT trunks) in a DT switch (that is, maximum number of servers supported)	144
Maximum number of switches that can be aggregated	2
Maximum number of physical links that can be aggregated in a single switch from a server (that is, maximum number of ports that can be in a trunk connected to a single switch)	4

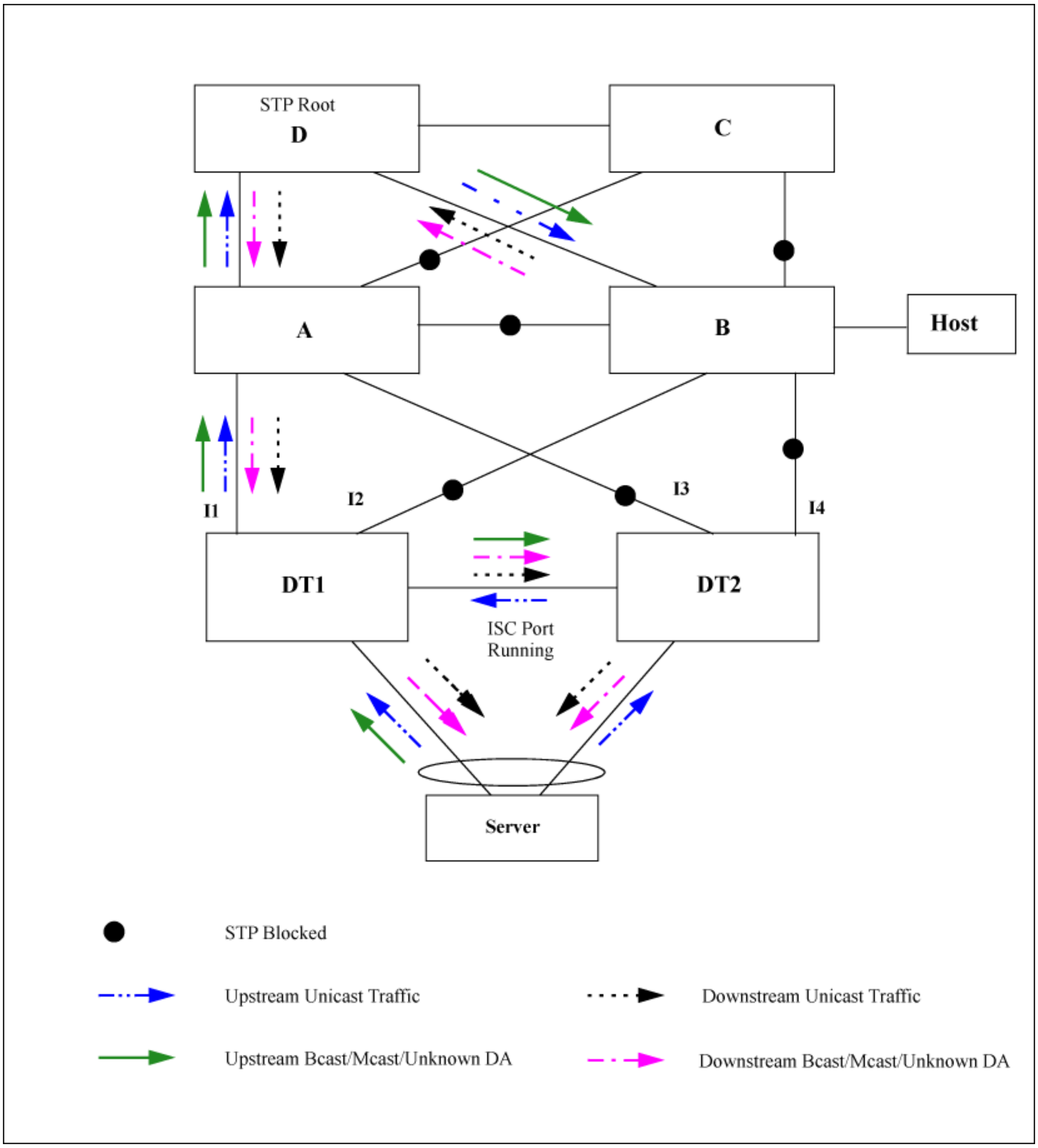
From the server perspective, this means that there could be a maximum total of 60 servers connected to two DT switches. Each server can have up to four physical links aggregated in a single switch, meaning that a single server could have a maximum of eight links (that is, four on each DT switch) in a DT trunk.

Forwarding traffic with distributed trunking and spanning tree

Refer to Figure 59 (page 135) for the following discussion about forwarding traffic when spanning tree is enabled. In this example, it is assumed that traffic is sent from a host off switch B to a server, and from the server back to the host. STP can block any one of the upstream links; in this example, STP has blocked all the links except the I1 link connected to DT1.

NOTE: STP is automatically disabled on the DT ports.

Figure 59 Example of distributed trunking with STP forwarding unicast, broadcast, and multicast traffic

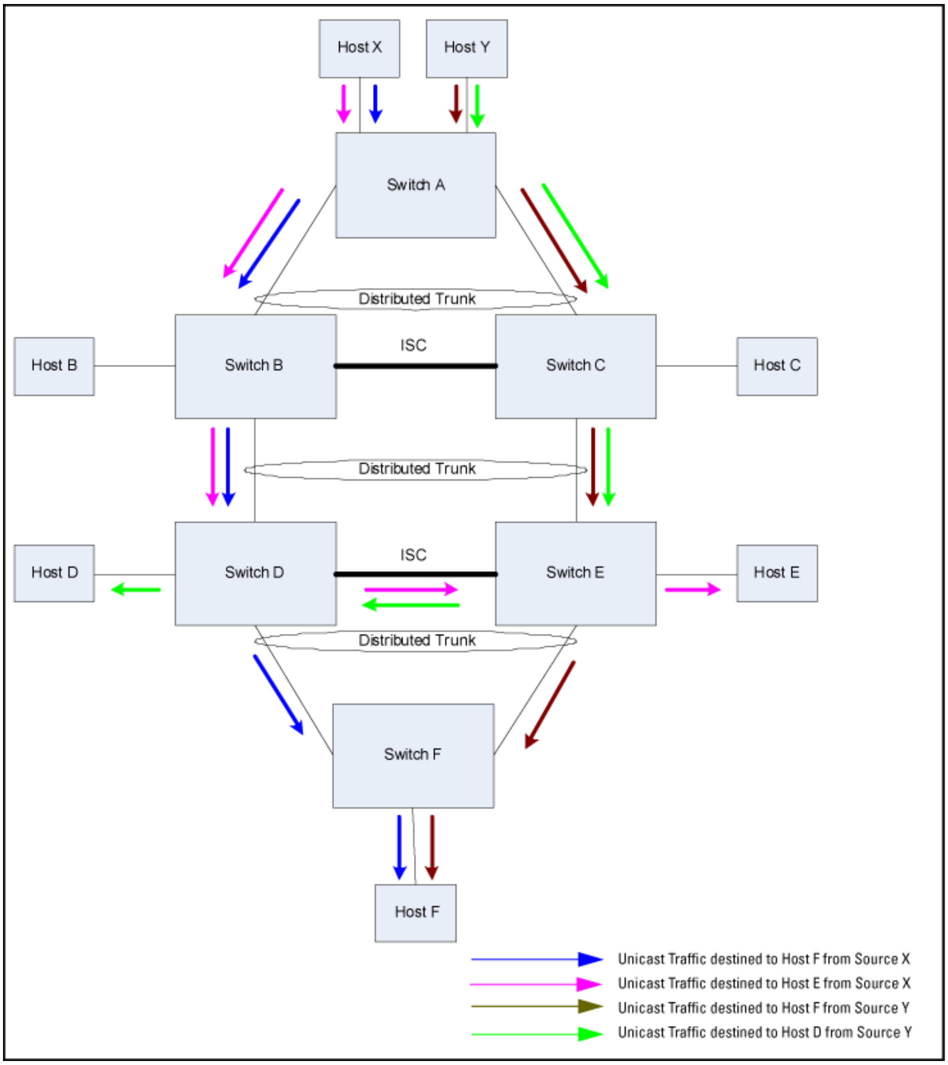

STP Root
D
C
A
B
Host
I1
I2
I3
I4
DT1
DT2
ISC Port
Running
Server
STP Blocked
Upstream Unicast Traffic
Downstream Unicast Traffic
Upstream Bcast/Mcast/Unknown DA
Downstream Bcast/Mcast/Unknown DA

Forwarding unicast traffic

Refer to Figure 60 (page 136) for the following discussion about forwarding traffic with switch-to-switch distributed trunking. Traffic from Host X or Y that is destined for Host F is always forwarded by Switch A over one of its standard 802.1AX trunk links to either Switch B or Switch C. When either Switch B or Switch C receives incoming traffic from Switch A, the traffic is directly forwarded to Switch F without traversing the ISC link.

Traffic from Host Y to Host D may go over the ISC if Switch A sends it to Switch C instead of sending it to Switch B.

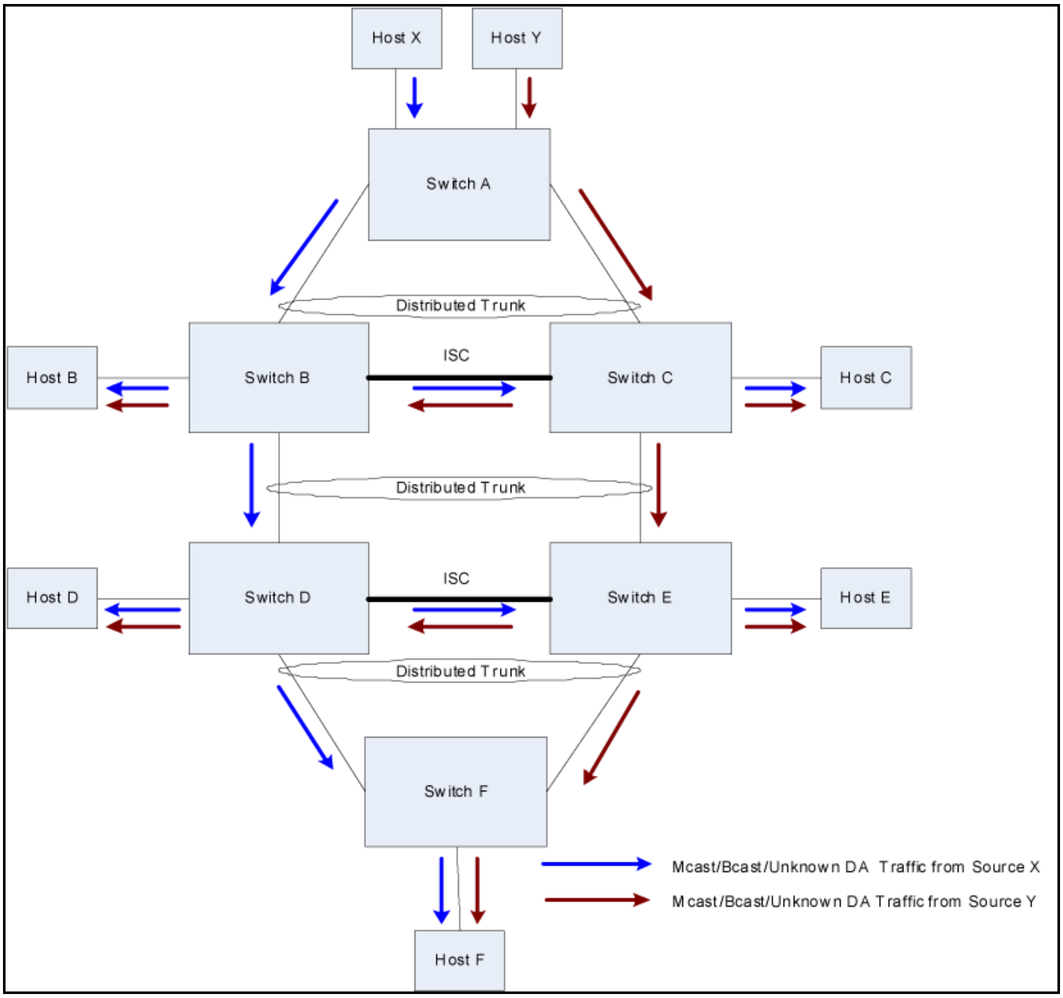
Figure 60 Unicast traffic flow across DT switches


Host X
Host Y
Switch A
Distributed Trunk
Host B
Switch B
ISC
Switch C
Host C
Distributed Trunk
Host D
Switch D
ISC
Switch E
Host E
Distributed Trunk
Switch F
Host F
Unicast Traffic destined to Host F from Source X
Unicast Traffic destined to Host E from Source X
Unicast Traffic destined to Host F from Source Y
Unicast Traffic destined to Host D from Source Y

Forwarding broadcast, multicast, and unknown traffic

In the example shown in Figure 61 (page 137), multicast/broadcast/unknown traffic from Host X or Y is always forwarded by Switch A over one of its standard 802.3ad trunk links to either Switch B or C. Switch B or C forwards the traffic on all the links including the ISC port, but not on the port that the traffic was received on. The peer DT switch (B or C) that receives broadcast/multicast/unknown traffic over the ISC port does not forward the packets to any of the DT trunks; the packet is sent only over the non-DT ports. The one exception is if the DT trunk on the peer aggregation device is down, then traffic received over the ISC is forwarded to the corresponding DT trunk.

Figure 61 Broadcast/multicast/unknown traffic flow access DT switches



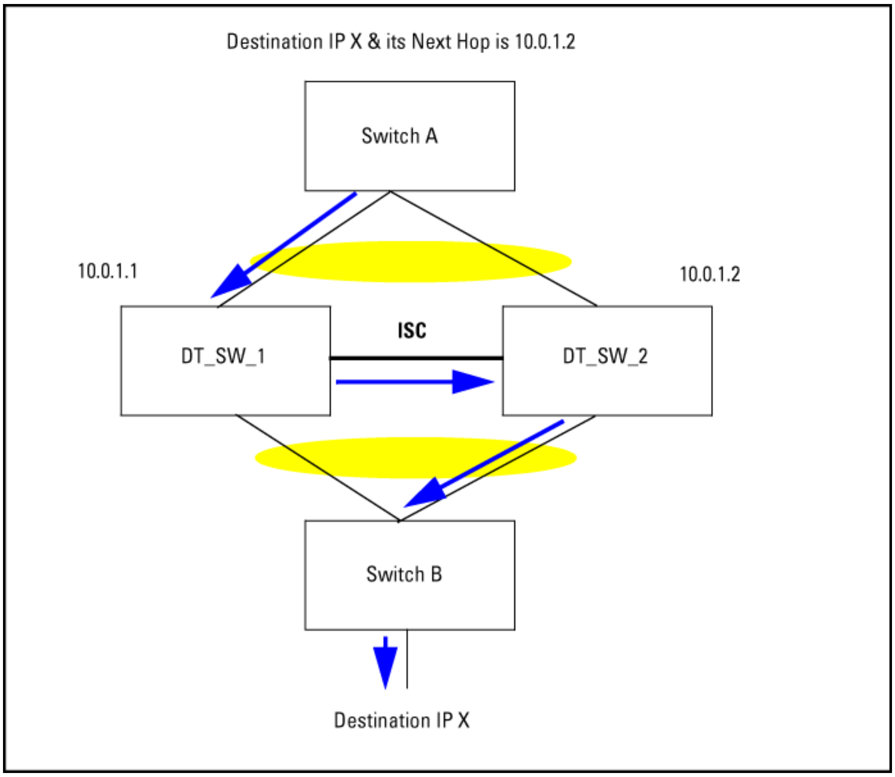
IP routing and distributed trunking

In switch-to-switch distributed trunking, the peer DT switches behave like independent Layer 3 devices with their own IP addresses in each active VLAN. If a DT switch receives a packet destined for the peer DT switch, it switches the packet through the ISC link. Interfaces on a VLAN using DT typically use a single default gateway pointing to only one of the DT switches in a DT pair.

The example in Figure 62 (page 138) shows Layer 3 (IP unicast) forwarding in a DT topology. The packet is sent as follows:

1. Switch A selects the link (using the trunk hash) to the DT pair. The packet is sent to the selected link DT_SW_1.
2. When DT_SW_1 receives the packet, it determines, based on the MAC address, that the packet must be sent over the ISC link to DT_SW_2.
3. When the packet arrives, DT_SW_2 performs a lookup and determines that the packet needs to be sent to Switch B.

Figure 62 Example 1 of layer 3 forwarding (IP unicast) in DT topology

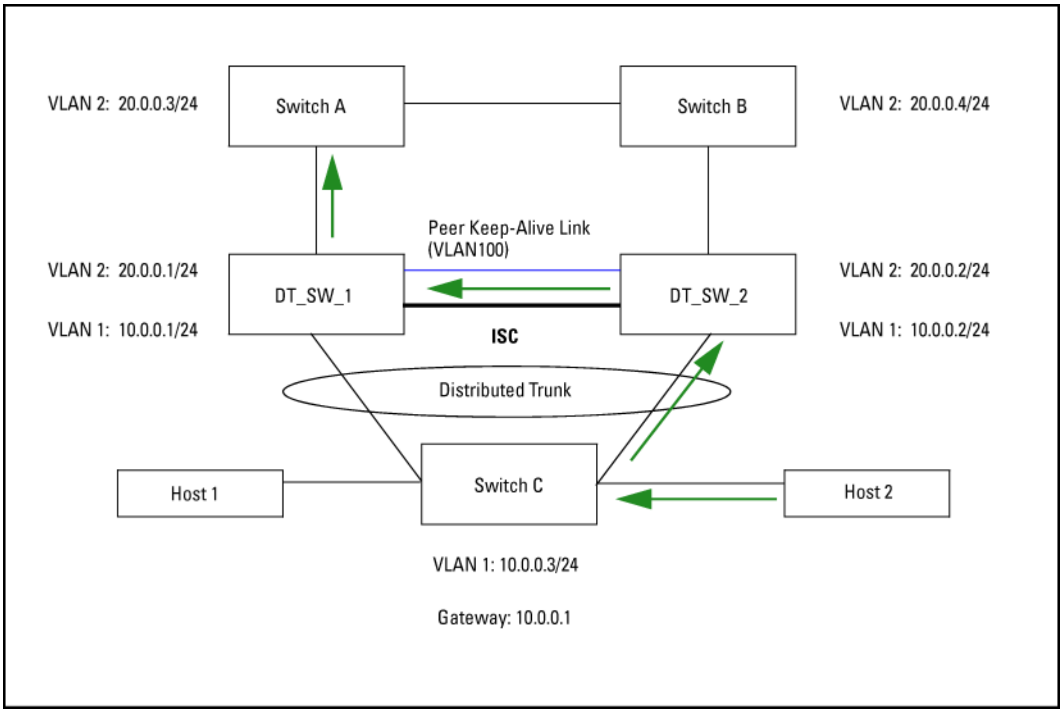


Another example in Figure 63 shows Layer 3 (IP unicast) forwarding in a DT topology. The packet is sent as follows:

1. Host 2 sends a packet to Switch C.
2. Switch C performs a lookup in the routing table and determines that the default gateway IP address is 10.0.0.1.
3. Layer 2 lookup determines that the outgoing interface is the DT port.
4. Hashing determines that the trunk member chosen is DT_SW_2 and the packet is sent there.
5. DT_SW_2 determines that the packet needs to be sent over the ISC link to DT_SW_1 based on the MAC address.
6. DT_SW_1 performs a lookup and determines that the packet goes to Switch A.

The packet is only forwarded if the outgoing interface is not a DT port, or if the outgoing DT port does not have an active interface on the peer switch.

Figure 63 Example 2 of layer 3 forwarding (IP unicast) in DT topology



Distributed trunking restrictions

There are several restrictions with distributed trunking:

Beginning with software version K.15.07, the switch will not allow both Distributed Trunking and MAC-based mirroring to function simultaneously. The switch will respond as follows:

- If the user attempts to configure both, an error message will appear.
- When a switch is updated from older software to K.15.07, if the older config file has both Distributed Trunking and MAC-based mirroring, the switch will automatically remove the MAC-based mirroring lines from the config file, and will give an explanatory error message.
- If a switch is running K.15.07 and an existing config file that has both Distributed Trunking and MAC-based mirroring is loaded onto the switch, the switch will automatically remove the MAC-based mirroring lines from the config file, and will give an explanatory error message.
- All DT linked switches must be running the same software version.
- The port trunk links should be configured manually (using manual LACP or manual trunks). Dynamic linking across switches is not supported.
- A distributed trunk can span a maximum of two switches.
- A maximum total of 144 servers can be connected to two DT switches. Each server can have up to four physical links aggregated in a single switch, meaning that there can be a maximum of eight ports (four aggregated links for each DT switch) included in a DT trunk.
- Only one ISC link is supported per switch, with a maximum of 60 DT trunks supported on the switch. The ISC link can be configured as a manual LACP trunk, non-protocol trunk, or as an individual link. Dynamic LACP trunks are not supported as ISCs.
- An ISC port becomes a member of all VLANs that are configured on the switch. When a new VLAN is configured, the ISC ports become members of that VLAN.
- Port trunk links can be done only on a maximum of two switches that are connected to a specific server.
- Any VLAN that is in a distributed trunk must be configured on both switches. By default, the distributed trunk belongs to the default VLAN.

- There can be eight links in a distributed trunk grouped across two switches, with a limit of four links per distributed trunking switch.
- The limit of 144 manual trunks per switch includes distributed trunks as well.
- ARP protection is not supported on the distributed trunks.
- Dynamic IP Lockdown protection is not supported on the distributed trunks.
- QinQ in mixed VLAN mode and distributed trunking are mutually exclusive.
- Features not supported include:
  - SVLANs in mixed mode on DT or ISC links
  - Meshing
  - CDP
  - GVRP
  - Multicast routing
  - IPv6 routing
  - MLD/MLD snooping on DT VLAN

DT operating notes when updating software versions

When updating software from a version that does not support DT Keepalive (prior to version K.15.03) to a version that supports shared DT keepalive (K.15.03 and greater), use the following procedure:

1. Disable the ISC interface on both switches, and then upgrade the software. Assume a2 is configured as switch-interconnect.

   ```
   HP Switch(config)# int a2 disable
   HP Switch(config)# write mem
   ```

2. Configure one of the existing uplink VLANs as a keepalive VLAN, and then configure the destination keepalive IP address (peer's keepalive IP address) on both switches at bootup.

   ```
   HP Switch(config)# distributed-trunking
   peer-keepalive vlan 2
   HP Switch(config)# distributed-trunking
   peer-keepalive destination 20.0.0.2
   ```

3. Ping the keepalive destination address to make sure that there is connectivity between the two DT switches (keepalive VLANs).
4. Enable the ISC link on both switches and then execute `write memory`. Assume a2 is configured as switch-interconnect.

   ```
   HP Switch(config)# int a2 enable
   HP Switch(config)# write mem
   ```

When updating software from a software version that does not support DT keepalive (prior to version K.15.03) to a version with dedicated point-to-point keepalive (K.15.03 and greater), use the following procedure:

1. Disable the ISC interface on both switches, and then upgrade the software. Assume a2 is configured as switch-interconnect.

   ```
   HP Switch(config)# int a2 disable
   HP Switch(config)# write mem
   ```

2. At switch bootup, create a dedicated VLAN for keepalive, and assign only the keepalive link port as a member port of the VLAN. Configure the keepalive destination IP address.

   ```
   HP Switch(config)# distributed-trunking
   peer-keepalive vlan 2
   ```

```
HP Switch(config)# distributed-trunking
peer-keepalive destination 20.0.0.2
```

3. Ping the keepalive destination address to make sure that there is connectivity between the two DT switches (keepalive VLANs).
4. Enable the ISC link on both switches, and then execute `write memory`. Assume a2 is configured as switch-interconnect.

```
HP Switch(config)# int a2 enable
HP Switch(config)# write mem
```

When updating software from a software version that does support shared DT keepalive (K.15.03, K.15.04) to a version that supports dedicated point-to-point keepalive (K.15.05), use the following procedure:

1. Disable the ISC interface and undo the keepalive configuration on both switches. Ignore the warning message that is displayed by the keepalive command while undoing the configuration. Upgrade the software. Assume a2 is configured as switch-interconnect.

```
HP Switch(config)# int a2 disable
HP Switch(config)# no distributed-trunking
peer-keepalive vlan
HP Switch(config)# write mem
```

2. At switch bootup, create a dedicated VLAN for keepalive and assign only the keepalive link port as a member port of the VLAN. Configure the keepalive destination IP address.

```
HP Switch(config)# vlan 10 (dedicated point-to-point VLAN interface)
HP Switch(vlan-10)#
HP Switch(vlan-10)# untagged b2 (keepalive link port)
HP Switch(vlan-10)# ip address 10.0.0.1/24
HP Switch(vlan-10)# exit
HP Switch(config)# distributed-trunking
peer-keepalive vlan 10
HP Switch(config)# distributed-trunking
peer-keepalive destination 10.0.0.2
```

3. Ping the keepalive destination address to make sure that there is connectivity between the two DT switches (keepalive VLANs).
4. Enable the ISC link on both switches, and then execute `write memory`. Assume a2 is configured as switch-interconnect.

```
HP Switch(config)# int a2 enable
HP Switch(config)# write mem
```

6 Port Traffic Controls

Command Summary

Table 19 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
[no] int *port-list* rate-limit all [in | out][percent *0-100* | kbps *0-10000000*]	Controls the rate of traffic sent or received on a port by setting a limit on the bandwidth available.	Disabled	(page 143)	-
show rate-limit all [port-list]	Displays the per-port rate-limit configuration in the running-config file.	-	(page 143)	-
[no] int *port- list* rate-limit icmp [percent *0-100* | kbps *0-10000000*]	Controls inbound usage of a port by setting a limit on the bandwidth available for inbound ICMP traffic.	Disabled	(page 145)	-
show rate-limit icmp [port-list]	Displays the per-interface ICMP rate-limit configuration in the running-config file.	-	(page 146)	-
setmib hpIcmpRatelimitPortAlarmflag.*internal-port-#* -i 1	Resets the ICMP trap function.	-	(page 146)	-
broadcast-limit *0-99*	Enables or disables broadcast limiting for outbound broadcasts on a selected port on the switch.	-	(page 147)	-
rate-limit [bcast | mcast]in percent *0-100* [no] rate-limit [bcast | mcast] in	Enables rate-limiting and sets limits for the specified inbound broadcast or multicast traffic.	Disabled	(page 148)	-
[no] int *port-list* bandwidth-min output	Configures the default minimum bandwidth allocation for the outbound priority queue for each port in*port-list*.	Defaults listed in this section	(page 149)	-
[no] int *port-list* bandwidth-min output [0-100 | strict]	Specifies the minimum outbound bandwidth as a percent of the total bandwidth for each outbound queue. The strict option provides the ability to configure the highest queue as strict.	-	(page 149)	-
show bandwidth output [port-list]	Displays the per-port GMB configuration in the running-config file.	-	(page 152)	-
show vlans	Lists the static VLANs configured on the switch.	-	(page 153)	-
show vlans ports *port-list*	Lists the static VLANs to which the specified ports belong, including the Jumbo column to indicate which VLANs are configured to support jumbo traffic.	-	(page 153)	-
show vlans *vid*	Shows port membership and jumbo configuration for the specified *vid*.	-	(page 153)	-

Table 19 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference

`vlan vid jumbo`
`[no]`
`vlan vid jumbo`
	Configures the specified VLAN to allow jumbo frames on all ports on the switch that belong to that VLAN.	Jumbos disabled on the specified VLAN	(page 155)	-

`jumbo max-frame-size size`	Sets the maximum frame size for jumbo frames.	9216 bytes	(page 155)	-
`jumbo ip-mtu size`	Globally sets the IP MTU size.	9198 bytes	(page 155)	-

Rate-limiting

In earlier releases, all traffic rate-limiting applied to inbound traffic only, and was specified as a percentage of total bandwidth. Beginning with software release K.12.xx or later, it is also possible to configure outbound rate-limiting for all traffic on a port and specify bandwidth usage in terms of kilobits per second (kbps).

△ **CAUTION: Rate-limiting is intended for use on edge ports in a network. It is not recommended for use on links to other switches, routers, or servers within a network, or for use in the network core. Doing so can interfere with applications the network requires to function properly.**

Configuring rate-limiting

Syntax:

```
[no] int port-list rate-limit all [ in | out ]  percent 0-100 | kbps
0-10000000
```

Configures a traffic rate limit (on non-trunked ports) on the link. The `no` form of the command disables rate-limiting on the specified ports.

The rate-limit all command controls the rate of traffic sent or received on a port by setting a limit on the bandwidth available. It includes options for:

- Rate-limiting on either inbound or outbound traffic.
- Specifying the traffic rate as either a percentage of bandwidth, or in terms of bits per second.

(Default: Disabled.)

`in` *or* `out`	Specifies a traffic rate limit on inbound traffic passing through that port, or on outbound traffic.
`percent` *or* `kbps`	Specifies the rate limit as a percentage of total available bandwidth, or in kilobits per second.

For more details on configuring rate-limiting, see "All traffic rate-limiting" (page 156).

Displaying the current rate-limit configuration

The `show rate-limit all` command displays the per-port rate-limit configuration in the running-config file.

Syntax:

```
show rate-limit all [port-list]
```

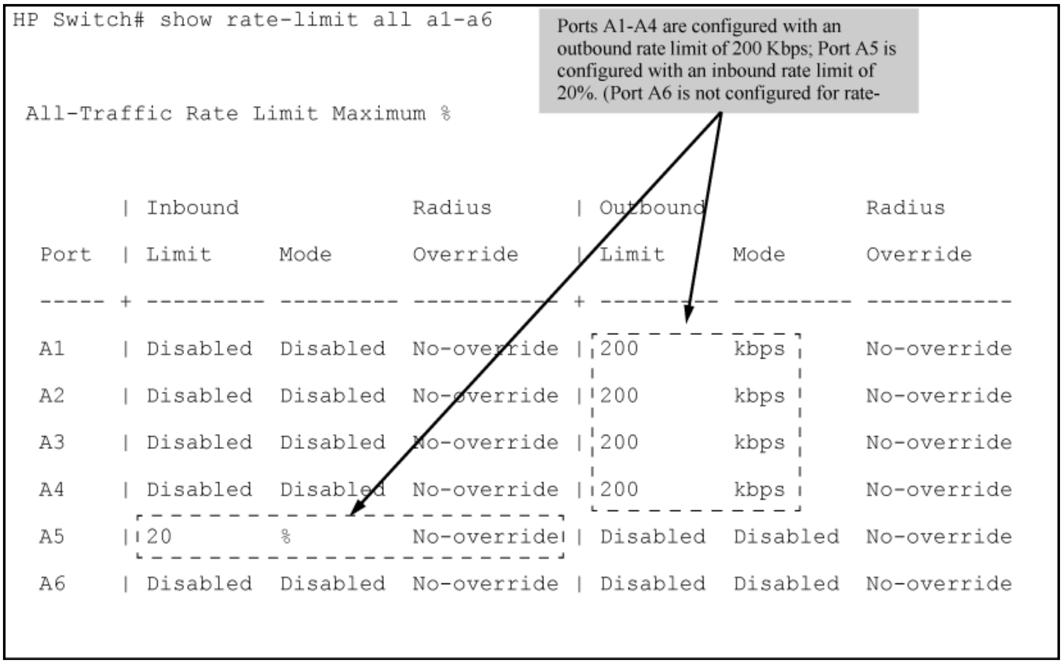
Without *`[port-list]`*, this command lists the rate-limit configuration for all ports on the switch.

With *`[port-list]`*, this command lists the rate-limit configuration for the specified ports. This command operates the same way in any CLI context.

Example

If you want to view the rate-limiting configuration on the first six ports in the module in slot "A":

Figure 64 Listing the rate-limit configuration



```
HP Switch# show rate-limit all a1-a6


 All-Traffic Rate Limit Maximum %


       | Inbound              Radius      | Outbound              Radius

  Port | Limit     Mode       Override    | Limit      Mode       Override

  ----- + --------- --------- ----------- + --------- --------- -----------

  A1   | Disabled  Disabled  No-override | 200        kbps       No-override

  A2   | Disabled  Disabled  No-override | 200        kbps       No-override

  A3   | Disabled  Disabled  No-override | 200        kbps       No-override

  A4   | Disabled  Disabled  No-override | 200        kbps       No-override

  A5   | 20        %         No-override | Disabled   Disabled   No-override

  A6   | Disabled  Disabled  No-override | Disabled   Disabled   No-override
```

Ports A1-A4 are configured with an outbound rate limit of 200 Kbps; Port A5 is configured with an inbound rate limit of 20%. (Port A6 is not configured for rate-

---

NOTE: To view **RADIUS**-assigned rate-limit information, use one of the following command options:

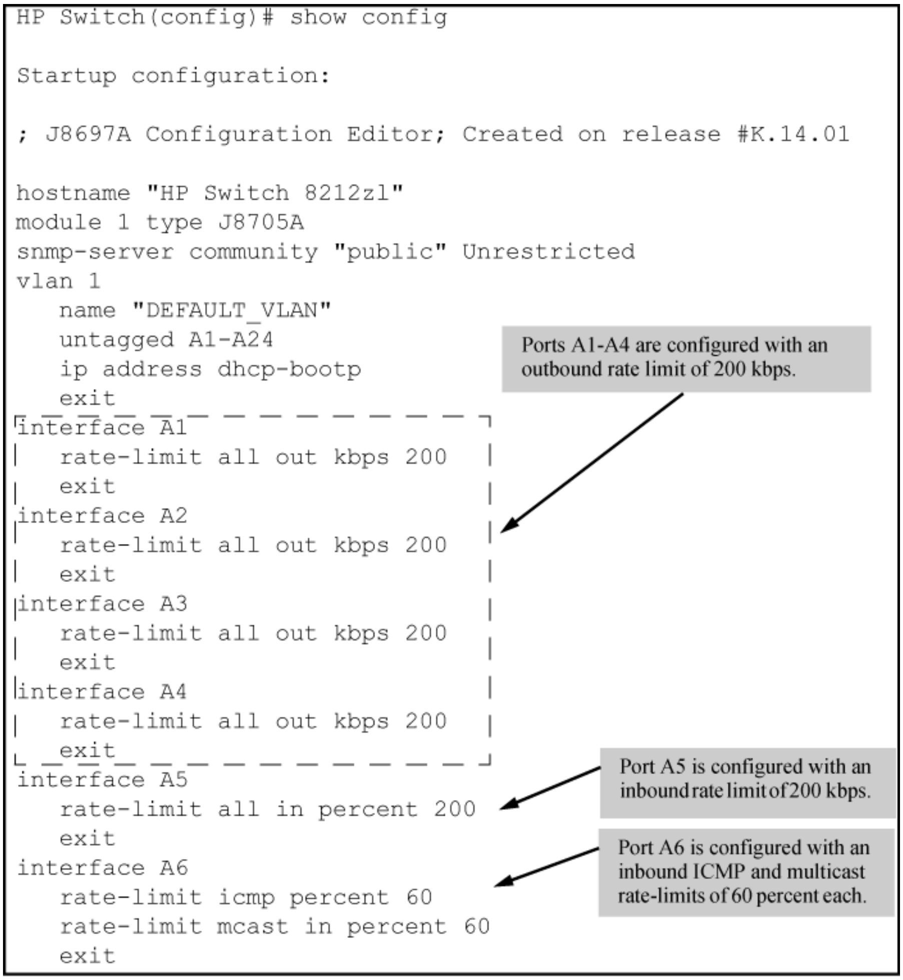
```
show port-access
    web-based clients port-list detailed
    mac-based clients port-list detailed
    authenticator clients port-list detailed
```

For more on **RADIUS**-assigned rate-limits, see the chapter titled "Configuring RADIUS Server Support for Switch Services" in the latest Management and Configuration Guide for your switch.

The `show running` command displays the currently applied setting for any interfaces in the switch configured for all traffic rate-limiting and ICMP rate limiting.

The `show config` command displays this information for the configuration currently stored in the `startup-config` file. (Note that configuration changes performed with the CLI, but not followed by a `write mem` command, do not appear in the `startup-config` file.)

Figure 65 Example of rate-limit settings listed in the `show config` output



```
HP Switch(config)# show config

Startup configuration:

; J8697A Configuration Editor; Created on release #K.14.01

hostname "HP Switch 8212zl"
module 1 type J8705A
snmp-server community "public" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A24
   ip address dhcp-bootp
   exit
interface A1
   rate-limit all out kbps 200
   exit
interface A2
   rate-limit all out kbps 200
   exit
interface A3
   rate-limit all out kbps 200
   exit
interface A4
   rate-limit all out kbps 200
   exit
interface A5
   rate-limit all in percent 200
   exit
interface A6
   rate-limit icmp percent 60
   rate-limit mcast in percent 60
   exit
```

Ports A1-A4 are configured with an outbound rate limit of 200 kbps.

Port A5 is configured with an inbound rate limit of 200 kbps.

Port A6 is configured with an inbound ICMP and multicast rate-limits of 60 percent each.

Configuring ICMP rate-limiting

For detailed information about ICMP rate-limiting, see "ICMP rate-limiting" (page 158).

The `rate-limit icmp` command controls inbound usage of a port by setting a limit on the bandwidth available for inbound ICMP traffic.

Syntax:

`[no] int` *`port- list`* `rate-limit icmp [ percent` *`0-100`* ` | kbps` *`0-10000000`* `]`

Configures inbound ICMP traffic rate-limiting. You can configure a rate limit from either the global configuration level (as shown above) or from the interface context level. The `no` form of the command disables ICMP rate-limiting on the specified interfaces.

(Default: Disabled.)

`percent` *`1-100`*	Values in this range allow ICMP traffic as a percentage of the bandwidth available on the interface.
`kbps` *`0-10000000`*	Specifies the rate at which to forward traffic in kilobits per second.
`0`	Causes an interface to drop all incoming ICMP traffic and is not recommended. See the *Caution* on 159.

Example

Either of the following commands configures an inbound rate limit of 1% on ports A3 to A5, which are used as network edge ports:

```
HP Switch(config) # int a3-a5 rate-limit icmp 1
HP Switch(eth-A3-A5) # rate-limit icmp 1
```

For information on using ICMP rate-limiting and all-traffic rate-limiting on the same interface, see“Using both ICMP rate-limiting and all-traffic rate-limiting on the same interface” (page 160).

Viewing the current ICMP rate-limit configuration

The `show rate-limit icmp` command displays the per-interface ICMP rate-limit configuration in the running-config file.

Syntax:

`show rate-limit icmp [port-list]`

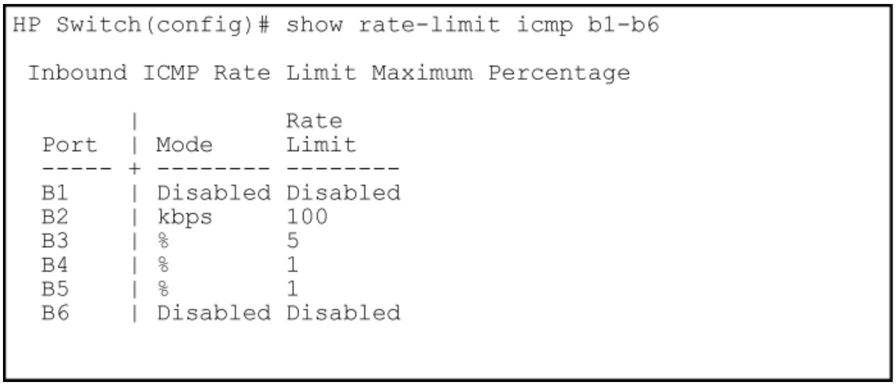
Without [*port-list*], this command lists the ICMP rate-limit configuration for all ports on the switch.

With [*port-list*], this command lists the rate-limit configuration for the specified interfaces. This command operates the same way in any CLI context

Example

If you want to view the rate-limiting configuration on the first six ports in the module in slot "B":

Figure 66 Listing the rate-limit configuration



```
HP Switch(config)# show rate-limit icmp b1-b6

 Inbound ICMP Rate Limit Maximum Percentage

        |          Rate
  Port  | Mode     Limit
  ----- + -------- --------
  B1    | Disabled Disabled
  B2    | kbps     100
  B3    | %        5
  B4    | %        1
  B5    | %        1
  B6    | Disabled Disabled
```

The `show running` command displays the currently applied setting for any interfaces in the switch configured for all traffic rate-limiting and ICMP rate-limiting.

The `show config` command displays this information for the configuration currently stored in the `startup-config` file. (Note that configuration changes performed with the CLI, but not followed by a `write mem` command, do not appear in the `startup-config` file.)

For more information on ICMP rate-limiting, see “Operating notes for ICMP rate-limiting” (page 161).

Resetting the ICMP trap function of the port

The port ICMP trap function can be reset through SNMP from a network management station or through the CLI with the `setmib` command. For information on ICMPrate-limiting trap and Event Log messages, see “ICMP rate-limiting trap and Event Log messages” (page 162).

Syntax:

`setmib hpIcmpRatelimitPortAlarmflag.`*`internal-port-#`*` -i 1`

On a port configured with ICMP rate-limiting, this command resets the ICMP trap function, which allows the switch to generate a new SNMP trap and an Event Log message if ICMP traffic in excess of the configured limit is detected on the port.

Example

An operator noticing an ICMP rate-limiting trap or Event Log message originating with port A1 on a switch would use the following `setmib` command to reset the port to send a new message if the condition occurs again:

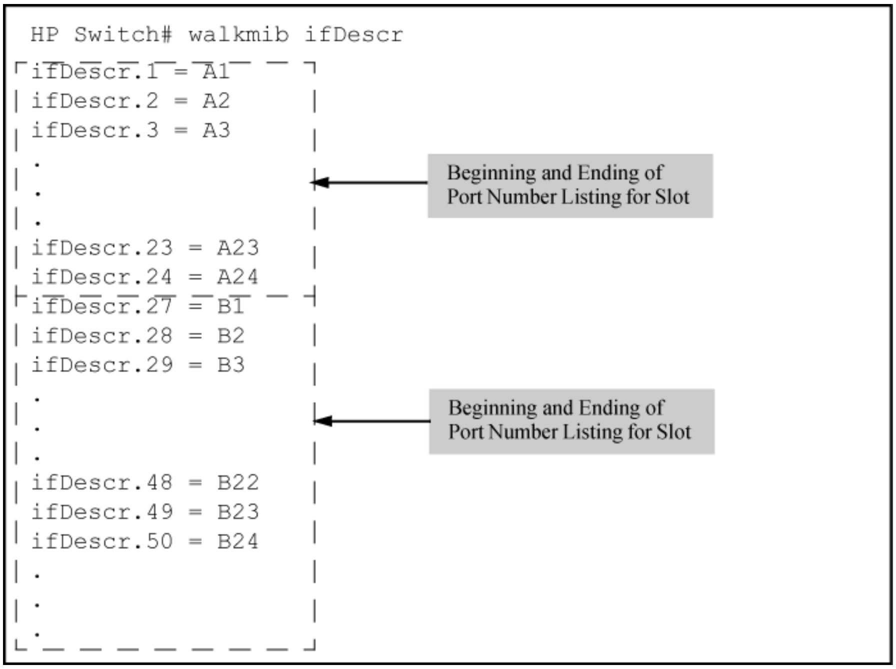
```
HP Switch(config)# setmib hpicmpratelimitportalarmflag.1 -i 1
```

Determining the switch port number used in ICMP port reset commands

To enable excess ICMP traffic notification traps and Event Log messages, use the `setmib` command described on (page 162). The port number included in the command corresponds to the internal number the switch maintains for the designated port and not the port's external (slot/number) identity.

To match the port's external slot/number to the internal port number, use the `walkmib ifDescr` command, as shown in the following figure:

Figure 67 Matching internal port numbers to external slot/port numbers



```
HP Switch# walkmib ifDescr
ifDescr.1 = A1
ifDescr.2 = A2
ifDescr.3 = A3
.
.
.
ifDescr.23 = A23
ifDescr.24 = A24
ifDescr.27 = B1
ifDescr.28 = B2
ifDescr.29 = B3
.
.
.
ifDescr.48 = B22
ifDescr.49 = B23
ifDescr.50 = B24
.
.
.
```

Beginning and Ending of Port Number Listing for Slot
Beginning and Ending of Port Number Listing for Slot

Configuring a broadcast limit on the switch

Broadcast limit on switches is configured on a per-port basis. You must be at the port context level for this command to work, for example:

```
HP Switch(config) # int B1
HP Switch(int B1) # broadcast-limit 1
```

Syntax:

`broadcast-limit [`*`0-99`*`]`

Enables or disables broadcast limiting for outbound broadcasts on a selected port on the switch.

The value selected is the percentage of traffic allowed, for example, `broadcast-limit 5` allows 5% of the maximum amount of traffic for that port. A value of zero disables broadcast limiting for that port.

NOTE: You must switch to port context level before issuing the `broadcast-limit` command. This feature is not appropriate for networks requiring high levels of IPX or RIP broadcast traffic.

Syntax:

`show config`

Displays the `startup-config` file. The broadcast limit setting appears here if enabled and saved to the `startup-config` file.

Syntax:

`show running-config`

Displays the `running-config` file. The broadcast limit setting appears here if enabled. If the setting is not also saved to the `startup-config` file, rebooting the switch returns broadcast limit to the setting currently in the `startup-config` file.

Example

The following command enables broadcast limiting of 1% of the traffic rate on the selected port on the switch:

```
HP Switch(int B1) # broadcast-limit 1
```

For a 1-Gbps port, this results in a broadcast traffic rate of 10 Mbps.

Configuring inbound rate-limiting for broadcast and multicast traffic

You can configure rate-limiting (throttling) of inbound broadcast and multicast traffic on the switch, which helps prevent the switch from being disrupted by traffic storms if they occur on the rate-limited port. The rate-limiting is implemented as a percentage of the total available bandwidth on the port.

The `rate-limit` command can be executed from the global or interface context, for example:

```
      HP Switch(config)# interface 3 rate-limit bcast in percent 10
```

or

```
      HP Switch(config)# interface 3
      HP Switch(eth-3)# rate-limit bcast in percent 10
```

Syntax:

`rate-limit [ bcast | mcast ] in percent` *`0-100`*
[no]
`rate-limit [ bcast | [mcast ]] in`

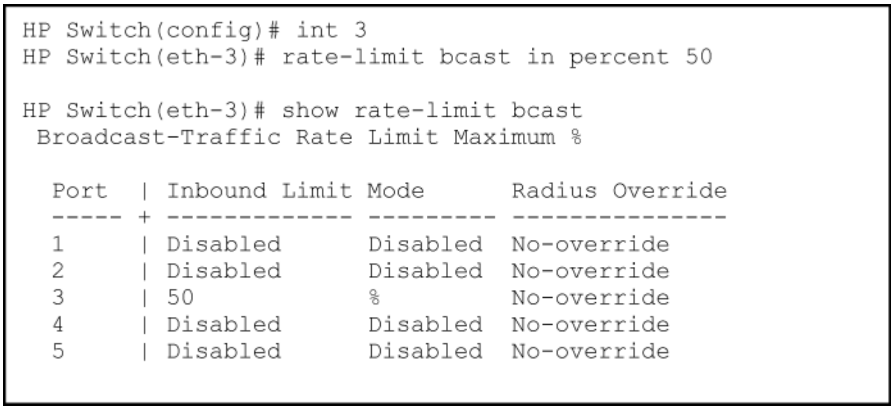
Enables rate-limiting and sets limits for the specified inbound broadcast or multicast traffic. Only the amount of traffic specified by the percent is forwarded.

Default: Disabled

Example

If you want to set a limit of 50% on inbound broadcast traffic for port 3, you can first enter interface context for port 3 and then execute the `rate-limit` command, as shown in Figure 68. Only 50% of the inbound broadcast traffic will be forwarded.

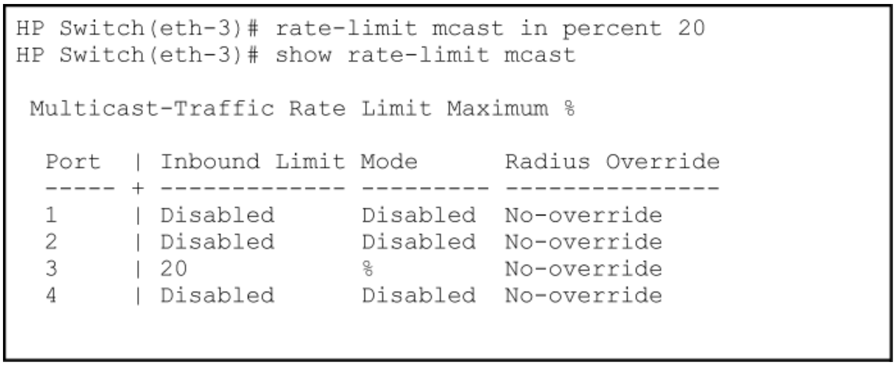
Figure 68 Inbound broadcast rate-limiting of 50% on port 3



```
HP Switch(config)# int 3
HP Switch(eth-3)# rate-limit bcast in percent 50

HP Switch(eth-3)# show rate-limit bcast
 Broadcast-Traffic Rate Limit Maximum %

   Port   | Inbound Limit Mode      Radius Override
   ----- + ------------- --------- ---------------
   1      | Disabled      Disabled  No-override
   2      | Disabled      Disabled  No-override
   3      | 50            %         No-override
   4      | Disabled      Disabled  No-override
   5      | Disabled      Disabled  No-override
```

If you rate-limit multicast traffic on the same port, the multicast limit is also in effect for that port, as shown in Figure 69. Only 20% of the multicast traffic will be forwarded.

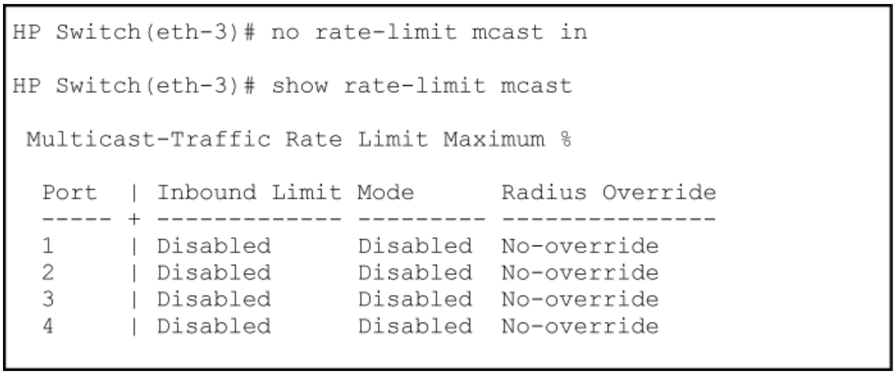
Figure 69 Example of Inbound multicast rate-limiting of 20% on port 3



```
HP Switch(eth-3)# rate-limit mcast in percent 20
HP Switch(eth-3)# show rate-limit mcast

 Multicast-Traffic Rate Limit Maximum %

   Port   | Inbound Limit Mode      Radius Override
   ----- + ------------- --------- ---------------
   1      | Disabled      Disabled  No-override
   2      | Disabled      Disabled  No-override
   3      | 20            %         No-override
   4      | Disabled      Disabled  No-override
```

To disable rate-limiting for a port enter the `no` form of the command, as shown in Figure 70.

Figure 70 Disabling inbound multicast rate-limiting for port 3



```
HP Switch(eth-3)# no rate-limit mcast in

HP Switch(eth-3)# show rate-limit mcast

 Multicast-Traffic Rate Limit Maximum %

   Port   | Inbound Limit Mode      Radius Override
   ----- + ------------- --------- ---------------
   1      | Disabled      Disabled  No-override
   2      | Disabled      Disabled  No-override
   3      | Disabled      Disabled  No-override
   4      | Disabled      Disabled  No-override
```

Operating Notes

- This rate-limiting option does not limit unicast traffic.
- This option does not include outbound multicast rate-limiting.

Configuring Guaranteed Minimum Bandwidth (GMB) for outbound traffic

For any port or group of ports you can configure either the default minimum bandwidth settings for each outbound priority queue or a customized bandwidth allocation. For most applications, HP recommends configuring GMB with the same values on all ports on the switch so that the outbound traffic profile is consistent for all outbound traffic. However, there may be instances where it may be advantageous to configure special profiles on connections to servers or to the network infrastructure (such as links to routers, other switches, or to the network core).

For detailed information about GMB, see "Guaranteed minimum bandwidth (GMB)" (page 162).

Syntax:

```
[no] int port-list bandwidth-min output
```

Configures the default minimum bandwidth allocation for the outbound priority queue for each port in the `port-list`. In the eight-queue configuration, the default values per priority queue are:

- Queue 1 (low priority): 2%
- Queue 2 (low priority): 3%
- Queue 3 (normal priority): 30%
- Queue 4 (normal priority): 10%
- Queue 5 (medium priority): 10%
- Queue 6 (medium priority): 10%
- Queue 7 (high priority): 15%
- Queue 8 (high priority): 20%

The no form of the command disables GMB for all ports in the `port-list`. In this state, which is the equivalent of setting all outbound queues on a port to **0** (zero), a high level of higher-priority traffic can starve lower-priority queues, which can slow or halt lower-priority traffic in the network.

You can configure bandwidth minimums from either the global configuration level (as shown above) or from the port context level. For information on outbound port queues, see "Per-port outbound priority queues" (page 163).

Syntax:

```
[no] int port-list bandwidth-min output [ 0-100 | strict ]
```

`[0-100]`
Select a minimum bandwidth.

For ports in `port-list`, specifies the minimum outbound bandwidth as a percent of the total bandwidth for each outbound queue. The queues receive service in descending order of priority.

You must specify a bandwidth percent value for all except the highest priority queue, which may instead be set to "strict" mode. The sum of the bandwidth percentages below the top queue cannot exceed 100%. (**0** is a value for a queue percentage setting.)

Configuring a total of less than 100% across the eight queues results in unallocated bandwidth that remains harmlessly unused unless a given queue becomes oversubscribed. In this case, the unallocated bandwidth is apportioned to oversubscribed queues in descending order of priority. For example, if you configure a minimum of 10% for queues 1 to 7 and 0% for queue 8, the unallocated bandwidth is available to all eight queues in the following prioritized order:

Queue 8 (high priority)
Queue 7 (high priority)
Queue 6 (medium priority)
Queue 5 (medium priority)
Queue 4 (normal priority)
Queue 3 (normal priority)
Queue 2 (low priority)
Queue 1 (low priority)

A setting of **0** (zero percent) on a queue means that no bandwidth minimum is specifically reserved for that queue for each of the ports in the `port-list`.

Also, there is no benefit to setting the high-priority queue (queue 8) to **0** (zero) unless you want the medium queue (queue 4) to be able to support traffic bursts above its guaranteed minimum.

`[strict]`
Provides the ability to configure the highest priority queue as strict. Per-queue values must be specified in priority order, with queue 1 having the lowest priority and queue 8 (or 4, or 2) having the highest priority (the highest queue is determined by how many queues are configured on the switch. Two, four, and eight queues are permitted. (See the `qos queue-config` command). The strict queue is provided all the bandwidth it needs. Any remaining bandwidth is shared among the non-strict queues based on need and configured bandwidth profiles (the profiles are applied to the leftover bandwidth in this case). The total sum of percentages for non-strict queues must not exceed 100.

NOTE: Configuring 0% for a queue can result in that queue being starved if any higher queue becomes over-subscribed and is then given all unused bandwidth.

The switch applies the bandwidth calculation to the link speed the port is currently using. For example, if a 10/100 Mbs port negotiates to 10 Mbps on the link, it bases its GMB calculations on 10 Mbps, not 100 Mbps.

Use `show bandwidth output` *`port-list`* to display the current GMB configuration. (The `show config` and `show running` commands do not include GMB configuration data.)

Example

For example, suppose you want to configure the following outbound minimum bandwidth availability for ports A1 and A2:

Priority of outbound port queue	Minimum bandwidth %	Effect on outbound bandwidth allocation
8	20%	Queue 8 has the first priority use of all outbound bandwidth not specifically allocated to queues 1 to 7. If, for example, bandwidth allocated to queue 5 is not being used and queues 7 and 8 become oversubscribed, queue 8 has first-priority use of the unused bandwidth allocated to queue 5.
7	15%	Queue 7 has a GMB of 15% available for outbound traffic. If queue 7 becomes oversubscribed and queue 8 is not already using all of the unallocated bandwidth, queue 7 can use the unallocated bandwidth. Also, any unused bandwidth allocated to queues 6 to queue 1 is available to queue 7 if queue 8 has not already claimed it.
6	10%	Queue 6 has a GMB of 10% and, if oversubscribed, is subordinate to queues 8 and 7 in priority for any unused outbound bandwidth available on the port.
5	10%	Queue 5 has a GMB of 10% and, if oversubscribed, is subordinate to queues 8, 7, and 6 for any unused outbound bandwidth available on the port.
4	10%	Queue 4 has a GMB of 10% and, if oversubscribed, is subordinate to queues, 8, 7, 6, and 5 for any unused outbound bandwidth available on the port.
3	30%	Queue 3 has a GMB of 30% and, if oversubscribed, is subordinate to queues, 8, 7, 6, 5, and 4 for any unused outbound bandwidth available on the port.

Priority of outbound port queue	Minimum bandwidth %	Effect on outbound bandwidth allocation
2	3%	Queue 2 has a GMB of 3% and, if oversubscribed, is subordinate to queues, 8, 7, 6, 5, 4, and 3 for any unused outbound bandwidth available on the port.
1	2%	Queue 1 has a GMB of 2% and, if oversubscribed, is subordinate to all the other queues for any unused outbound bandwidth available on the port.

Either of the following commands configures ports A1 through A5 with bandwidth settings:

```
HP Switch(config) # int a1-a5 bandwidth-min output 2 3 30 10 10 10 15 strict
HP Switch(eth-A1-A5) # bandwidth-min output 2 3 30 10 10 10 15 strict
```

Viewing the current GMB configuration

This command displays the per-port GMB configuration in the `running-config` file.

Syntax:

`show bandwidth output` [`port-list`]

Without *`port-list`*, this command lists the GMB configuration for all ports on the switch.

With *`port-list`*, this command lists the GMB configuration for the specified ports.

This command operates the same way in any CLI context. If the command lists `Disabled` for a port, there are no bandwidth minimums configured for any queue on the port. (See the description of the no form of the `bandwidth-min output` command on page 13-24.)

Example

To display the GMB configuration resulting from either of the above commands:

Figure 71 Listing the GMB configuration

```
HP Switch(config)# show bandwidth output a1-a5

 Outbound Guaranteed Minimum Bandwidth %

  Port   Q1  Q2     Q3  Q4     Q5  Q6  Q7  Q8
  ------ --- ------ --- ------ --- --- --- ------
  A1     2   3      30  10     10  10  15  strict
  A2     2   3      30  10     10  10  15  strict
  A3     2   3      30  10     10  10  15  strict
  A4     2   3      30  10     10  10  15  strict
  A5     2   3      30  10     10  10  15  strict
```

This is how the preceding listing of the GMB configuration would appear in the `startup-config` file.

Figure 72 GMB settings listed in the `show config` output

```
HP Switch(config)# show config status
Running configuration is same as the startup configuration
HP Switch(config)# show config

Startup configuration:
; J9091A configuration Editor; Created on release #K.15.05.0000x

hostnme “HP Switch”
module 1 type J8697A
snmp-server community “public” Unrestricted
vlan 1
   name “DEFAULT_VLAN”
   untagged A1-A24
   ip address dhcp-bootp
   exit
interface A1
   bandwidth-min output 2 3 30 10 10 10 15 strict
   exit
interface A2
   bandwidth-min output 2 3 30 10 10 10 15 strict
   exit
interface A3
   bandwidth-min output 2 3 30 10 10 10 15 strict
   exit
interface A4
   bandwidth-min output 2 3 30 10 10 10 15 strict
   exit
interface A5
   bandwidth-min output 2 3 30 10 10 10 15 strict
   exit
```

Configuring jumbo frame operation

For detailed information about jumbo frames, see “Jumbo frames” (page 164).

Overview

1. Determine the VLAN membership of the ports or trunks through which you want the switch to accept inbound jumbo traffic. For operation with GVRP enabled, refer to the GVRP topic under “Operating Rules”, above.
2. Ensure that the ports through which you want the switch to receive jumbo frames are operating at least at gigabit speed. (Check the Mode field in the output for the `show interfaces brief` *`port-list`* command.)
3. Use the `jumbo` command to enable jumbo frames on one or more VLANs statically configured in the switch. (All ports belonging to a jumbo-enabled VLAN can receive jumbo frames.
4. Execute `write memory` to save your configuration changes to the `startupconfig` file.

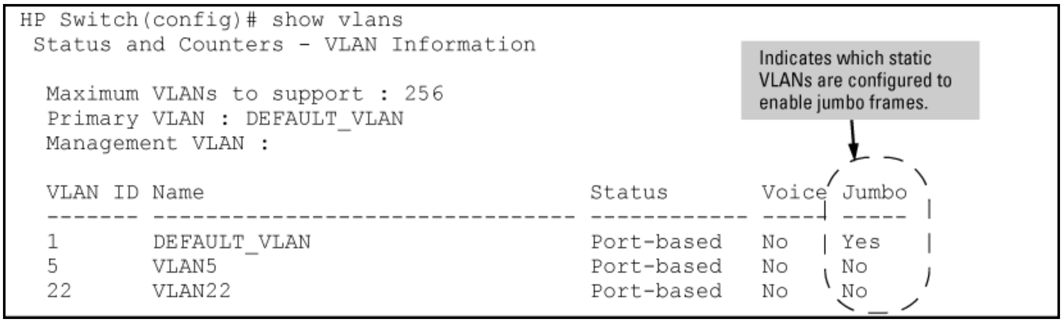
Viewing the current jumbo configuration

Syntax:

`show vlans`

Lists the static VLANs configured on the switch and includes a Jumbo column to indicate which VLANs are configured to support inbound jumbo traffic. All ports belonging to a jumbo-enabled VLAN can receive jumbo traffic. (For more information, see “Configuring a maximum frame size” (page 155).) See Figure Figure 73.

Figure 73 Example listing of static VLANs to show jumbo status per VLAN



```
HP Switch(config)# show vlans
 Status and Counters - VLAN Information

  Maximum VLANs to support : 256
  Primary VLAN : DEFAULT_VLAN
  Management VLAN :

  VLAN ID Name                             Status       Voice  Jumbo
  ------- -------------------------------- ------------ -----  -----
  1       DEFAULT_VLAN                     Port-based   No     Yes
  5       VLAN5                            Port-based   No     No
  22      VLAN22                           Port-based   No     No
```

Indicates which static VLANs are configured to enable jumbo frames.

Syntax:

`show vlans ports` *`port-list`*

Lists the static VLANs to which the specified ports belong, including the `Jumbo` column to indicate which VLANs are configured to support jumbo traffic.

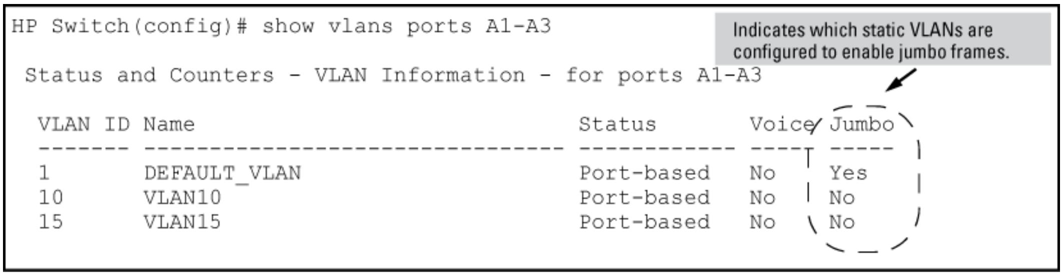
Entering only one port in *`port-list`* results in a list of all VLANs to which that port belongs.

Entering multiple ports in *`port-list`* results in a superset list that includes the VLAN memberships of all ports in the list, even though the individual ports in the list may belong to different subsets of the complete VLAN listing.

Example

If port 1 belongs to VLAN 1, port 2 belongs to VLAN 10, and port 3 belongs to VLAN 15, executing this command with a *`port-list`* of **1 - 3** results in a listing of all three VLANs, even though none of the ports belong to all three VLANS. (See Figure 74.)

Figure 74 Listing the VLAN memberships for a range of ports



```
HP Switch(config)# show vlans ports A1-A3

 Status and Counters - VLAN Information - for ports A1-A3

  VLAN ID Name                             Status       Voice  Jumbo
  ------- -------------------------------- ------------ -----  -----
  1       DEFAULT_VLAN                     Port-based   No     Yes
  10      VLAN10                           Port-based   No     No
  15      VLAN15                           Port-based   No     No
```

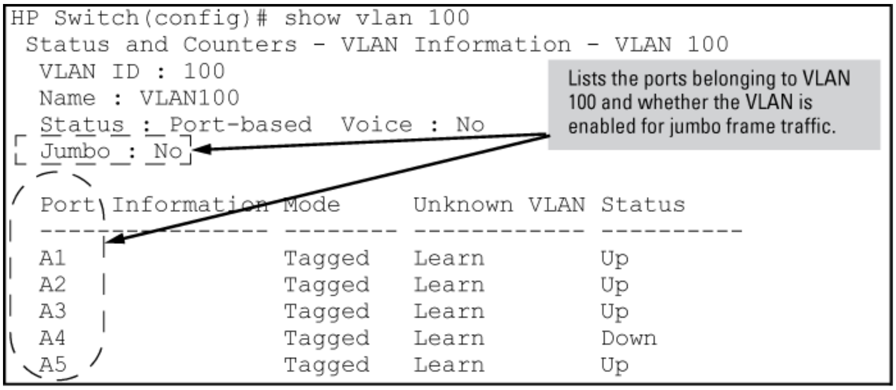
Indicates which static VLANs are configured to enable jumbo frames.

Syntax:

`show vlans` *`vid`*

Shows port membership and jumbo configuration for the specified *`vid`* . (See Figure 75.)

Figure 75 Example of listing the port membership and jumbo status for a VLAN



```
HP Switch(config)# show vlan 100
 Status and Counters - VLAN Information - VLAN 100
  VLAN ID : 100
  Name : VLAN100
  Status : Port-based  Voice : No
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  A1               Tagged   Learn        Up
  A2               Tagged   Learn        Up
  A3               Tagged   Learn        Up
  A4               Tagged   Learn        Down
  A5               Tagged   Learn        Up
```

Lists the ports belonging to VLAN 100 and whether the VLAN is enabled for jumbo frame traffic.

Enabling or disabling jumbo traffic on a VLAN

Syntax:

```
vlan vid jumbo
no vlan vid jumbo
```

Configures the specified VLAN to allow jumbo frames on all ports on the switch that belong to that VLAN. If the VLAN is not already configured on the switch, `vlan` *`vid`* `jumbo` also creates the VLAN.

A port belonging to one jumbo VLAN can receive jumbo frames through any other VLAN statically configured on the switch, regardless of whether the other VLAN is enabled for jumbo frames.

The `[no]` form of the command disables inbound jumbo traffic on all ports in the specified VLAN that do not also belong to another VLAN that is enabled for jumbo traffic. In a VLAN context, the command forms are `jumbo` and `no jumbo`.

(Default: Jumbos disabled on the specified VLAN.)

Configuring a maximum frame size

You can globally set a maximum frame size for jumbo frames that will support values from 1518 bytes to 9216 bytes for untagged frames.

Syntax:

```
jumbo max-frame-size size
```

Sets the maximum frame size for jumbo frames. The range is from 1518 bytes to 9216 bytes. (Default: 9216 bytes)

NOTE: The jumbo `max-frame-size` is set on a GLOBAL level.

Configuring IP MTU

NOTE: The following feature is available on the switches covered in this guide. `jumbos` support is required for this feature. On switches that do not support this command, the IP MTU value is derived from the maximum frame size and is not configurable.

You can set the IP MTU globally by entering this command. The value of `max-frame-size` must be greater than or equal to 18 bytes more than the value selected for `ip-mtu`. For example, if `ip-mtu` is set to 8964, the `max-frame-size` is configured as 8982.

Syntax:

```
jumbo ip-mtu size
```

Globally sets the IP MTU size. Values range between 1500 and 9198 bytes. This value must be 18 bytes less than the value of `max-frame-size`.

(Default: 9198 bytes)

Displaying the maximum frame size

Use the `show jumbos` command to display the globally configured untagged maximum frame size for the switch, as shown in the following example.

```
HP Switch(config)# show jumbos

 Jumbos Global Values

  Configured : MaxFrameSize : 9216   Ip-MTU : 9198
  In Use     : MaxFrameSize : 9216   Ip-MTU : 9198
```

For more information about frame size, see “Jumbo frames” (page 164).

Operating notes for maximum frame size

- When you set a maximum frame size for jumbo frames, it must be on a global level. You cannot use the `jumbo max-frame-size` command on a per-port or per-VLAN basis.
- The original way to configure jumbo frames remains the same, which is per-VLAN, but you cannot set a maximum frame size per-VLAN.
- Jumbo support must be enabled for a VLAN from the CLI or through SNMP.
- Setting the maximum frame size does not require a reboot.
- When you upgrade to a version of software that supports setting the maximum frame size from a version that did not, the `max-frame-size` value is set automatically to 9216 bytes.
- Configuring a jumbo maximum frame size on a VLAN allows frames up to `max-frame-size` even though other VLANs of which the port is a member are not enabled for jumbo support.

All traffic rate-limiting

Rate-limiting for all traffic operates on a per-port basis to allow only the specified bandwidth to be used for inbound or outbound traffic. When traffic exceeds the configured limit, it is dropped. This effectively sets a usage level on a given port and is a tool for enforcing maximum service level commitments granted to network users. This feature operates on a per-port level and is not configurable on port trunks. Rate-limiting is designed to be applied at the network edge to limit traffic from non-critical users or to enforce service agreements such as those offered by Internet Service Providers (ISPs) to provide only the bandwidth for which a customer has paid.

△ **CAUTION: Rate-limiting is intended for use on edge ports in a network. HP does not recommend it for use on links to other switches, routers, or servers within a network, or for use in the network core. Doing so can interfere with applications the network requires to function properly.**

NOTE: Rate-limiting also can be applied by a RADIUS server during an authentication client session. For further details, see the chapter "*RADIUS Authentication and Accounting*" in the *Access Security Guide* for your switch.

The switches also support ICMP rate-limiting to mitigate the effects of certain ICMP-based attacks. For more information, see "ICMP rate-limiting" (page 158).

The mode using bits per second (bps) in releases before K.12.XX has been replaced by the kilobits per second (kbps) mode. Switches that have configurations with bps values are automatically converted when you update your software to the new version. However, you must manually update to kbps values an older config file that uses bps values or it will not load successfully onto a switch running later versions of the software (K.12.XX or greater).

- The `rate-limit icmp` command specifies a rate limit on inbound ICMP traffic only (See "ICMP Rate-Limiting" on page 13-9)
- Rate-limiting does not apply to trunked ports (including meshed ports).
- Kbps rate-limiting is done in segments of 1% of the lowest corresponding media speed.

  For example, if the media speed is 100 Kbps, the value would be 1 Mbps.

  - A 1 to 100 Kbps rate-limit is implemented as a limit of 100 Kbps
  - A limit of 100 to 199 Kbps is also implemented as a limit of 100 Kbps.
  - A limit of 200 to 299 Kbps is implemented as a limit of 200 Kbps, and so on.
- Percentage limits are based on link speed.

  For example, if a 100 Mbps port negotiates a link at 100 Mbps and the inbound rate-limit is configured at 50%, the traffic flow through that port is limited to no more than 50 Mbps.

Similarly, if the same port negotiates a 10 Mbps link, it allows no more than 5 Mbps of inbound traffic.

- Configuring a rate limit of 0 (zero) on a port blocks all traffic on that port. However, if this is the desired behavior on the port, HP Switch recommends that you use the *`port-list`* `disable` command instead of configuring a rate limit of 0.
- You can configure a rate limit from either the global configuration level or from the port context level.

Example

Either of the following commands configures an inbound rate limit of 60% on ports A3 to A5:

```
HP Switch (config) # int a3-a5 rate-limit all in percent 60
HP Switch (eth-A3-A5)# rate-limit all in percent 60
```

Operating notes for rate-limiting

- Rate-limiting operates on a per-port basis, regardless of traffic priority. Rate-limiting is available on all types of ports (other than trunked ports) and at all port speeds configurable for these switches.
- Rate-limiting is not allowed on trunked ports. Rate-limiting is not supported on ports configured in a trunk group (including mesh ports). Configuring a port for rate-limiting and then adding it to a trunk suspends rate-limiting on the port while it is in the trunk. Attempting to configure rate-limiting on a port that already belongs to a trunk generates the following message:

  `port-list`: `Operation is not allowed for a trunked port.`
- Rate-limiting for inbound and outbound traffic are separate features. The rate limits for each direction of traffic flow on the same port are configured separately—even the specified limits can be different.
- Rate-limiting and hardware: The hardware will round the actual Kbps rate down to the nearest multiple of 64 Kbps.
- Rate-limiting is visible as an outbound forwarding rate. Because inbound rate-limiting is performed on packets during packet-processing, it is not shown via the inbound drop counters. Instead, this limit is verifiable as the ratio of outbound traffic from an inbound rate-limited port versus the inbound rate. For outbound rate-limiting, the rate is visible as the percentage of available outbound bandwidth (assuming that the amount of requested traffic to be forwarded is larger than the rate-limit).
- Operation with other features: Configuring rate-limiting on a port where other features affect port queue behavior (such as flow control) can result in the port not achieving its configured rate-limiting maximum. For example, in a situation whereflow control is configured on a rate-limited port, there can be enough "back pressure" to hold high-priority inbound traffic from the upstream device or application to a rate that is lower than the configured rate limit. In this case, the inbound traffic flow does not reach the configured rate and lower priority traffic is not forwarded into the switch fabric from the rate-limited port. (This behavior is termed "head-of-line blocking" and is a well-known problem with flow-control.)

  In another type of situation, an outbound port can become oversubscribed by traffic received from multiple rate-limited ports. In this case, the actual rate for traffic on the rate-limited ports may be lower than configured because the total traffic load requested to the outbound port exceeds the port's bandwidth, and thus some requested traffic may be held off on inbound.
- Traffic filters on rate-limited ports. Configuring a traffic filter on a port does not prevent the switch from including filtered traffic in the bandwidth-use measurement for rate-limiting when it is configured on the same port. For example, ACLs, source-port filters, protocol filters, and multicast filters are all included in bandwidth usage calculations.

- Monitoring (mirroring) rate-limited interfaces.If monitoring is configured, packets dropped by rate-limiting on a monitored interface are still forwarded to the designated monitor port. (Monitoring shows what traffic is inbound on an interface, and is not affected by "drop" or "forward" decisions.)
- Optimum rate-limiting operation. Optimum rate-limiting occurs with 64-byte packet sizes. Traffic with larger packet sizes can result in performance somewhat below the configured bandwidth. This is to ensure the strictest possible rate-limiting of all sizes of packets.

NOTE: Rate-limiting is applied to the available bandwidth on a port and not to any specific applications running through the port. If the total bandwidth requested by all applications is less than the configured maximum rate, then no rate-limit can be applied. This situation occurs with a number of popular throughput-testing applications, as well as most regular network applications. Consider the following example that uses the minimum packet size:

The total available bandwidth on a 100 Mbps port "X" (allowing for Inter-packet Gap—IPG), with no rate-limiting restrictions, is:

```
(((100,000,000 bits) / 8 ) / 84) × 64 = 9,523,809 bytes per
second
```

where:

- The divisor (84) includes the 12-byte IPG, 8-byte preamble, and 64-bytes of data required to transfer a 64-byte packet on a 100 Mbps link.
- Calculated "bytes-per-second" includes packet headers and data. This value is the maximum "bytes-per-second" that 100 Mbps can support for minimum-sized packets.

Suppose port "X" is configured with a rate limit of 50% (4,761,904 bytes). If a throughput-testing application is the only application using the port and transmits 1 Mbyte of data through the port, it uses only 10.5% of the port's available bandwidth, and the rate-limit of 50% has no effect. This is because the maximum rate permitted (50%) exceeds the test application's bandwidth usage (126,642-164,062 bytes, depending upon packet size, which is only 1.3% to 1.7% of the available total). Before rate-limiting can occur, the test application's bandwidth usage must exceed 50% of the port's total available bandwidth. That is, to test the rate-limit setting, the following must be true:

```
bandwidth usage (0.50 × 9,523,809)
```

ICMP rate-limiting

As of software version K.15.02.0004, ICMP rate-limiting and classifier-based-rate-limiting operates on the entire packet length instead of just the IP payload part of the packet. As a result, the effective metering rate is now the same as the configured rate. The rate-limiting applies to these modules:

HP device	Product number	Minimum supported software version
HP Switch 24-port 10/100/1000 PoE+ v2 zl Module	J9534A	K.15.02.0004
HP Switch 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module	J9535A	K.15.02.0004
HP Switch 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module	J9536A	K.15.02.0004
HP Switch 24-port SFP v2 zl Module	J9537A	K.15.02.0004
HP Switch 8-port 10-GbE SFP+ v2 zl Module	J9538A	K.15.02.0004
HP 24-port 10/100 PoE+ v2 zl Module	J9547A	K.15.02.0004

HP device	Product number	Minimum supported software version
HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module	J9548A	K.15.02.0004
HP 20-port Gig-T / 4-port SFP v2 zl Module	J9549A	K.15.02.0004
HP 24-port Gig-T v2 zl Module	J9550A	K.15.02.0004
HP 12-port Gig-T / 12-port SFP v2 zl Module	J9637A	K.15.02.0004

In IP networks, ICMP messages are generated in response to either inquiries or requests from routing and diagnostic functions. These messages are directed to the applications originating the inquiries. In unusual situations, if the messages are generated rapidly with the intent of overloading network circuits, they can threaten network availability. This problem is visible in denial-of-service (DoS) attacks or other malicious behaviors where a worm or virus overloads the network with ICMP messages to an extent where no other traffic can get through. (ICMP messages themselves can also be misused as virus carriers). Such malicious misuses of ICMP can include a high number of ping packets that mimic a valid source IP address and an invalid destination IP address (spoofed pings), and a high number of response messages (such as Destination Unreachable error messages) generated by the network.

ICMP rate-limiting provides a method for limiting the amount of bandwidth that may be used for inbound ICMP traffic on a switch port or trunk. This feature allows users to restrict ICMP traffic to percentage levels that permit necessary ICMP functions, but throttle additional traffic that may be caused by worms or viruses (reducing their spread and effect). In addition, ICMP rate-limiting preserves inbound port bandwidth for non-ICMP traffic.

△ **CAUTION:** This feature should not be used to remove all ICMP traffic from a network. ICMP is necessary for routing, diagnostic, and error responses in an IP network. ICMP rate-limiting is primarily used for throttling worm or virus-like behavior and should normally be configured to allow one to five percent of available inbound bandwidth (at 10 Mbps or 100 Mbps speeds) or 100 to 10,000 kbps (1Gbps or 10 Gbps speeds) to be used for ICMP traffic.

NOTE: ICMP rate-limiting does not throttle non-ICMP traffic. In cases where you want to throttle both ICMP traffic and all other inbound traffic on a given interface, you can separately configure both ICMP rate-limiting and all-traffic rate-limiting.

Beginning with software release K.12.xx or later, the all-traffic rate-limiting command (`rate-limit all`) and the ICMP rate-limiting command (`rate-limit icmp`) operate differently:

- All-traffic rate-limiting applies to both inbound and outbound traffic and can be specified either in terms of a percentage of total bandwidth or in terms of bits per second;
- ICMP rate-limiting applies only to inbound traffic and can be specified as only a percentage of total bandwidth.

ICMP rate-limiting is not supported on meshed ports. (Rate-limiting can reduce the efficiency of paths through a mesh domain).

Terminology

All-traffic rate-limiting: Applies a rate-limit to all traffic (including ICMP traffic) on an interface. For details, see "Rate-limiting" (page 143).

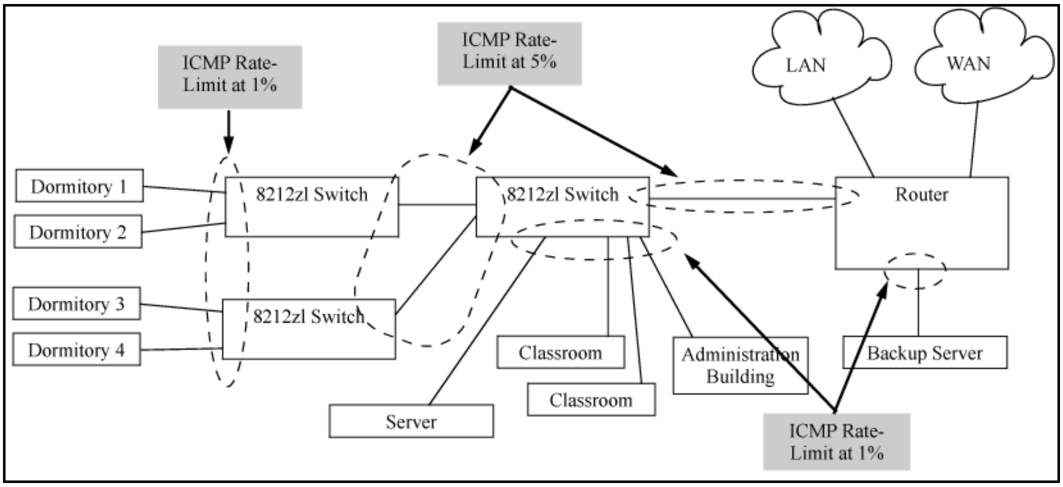
ICMP rate-limiting: Applies a rate-limit to all inbound ICMP traffic received on an interface, but does not limit other types of inbound traffic.

Spoofed ping: An ICMP echo request packet intentionally generated with a valid source IP address and an invalid destination IP address. Spoofed pings are often created with the intent to oversubscribe network resources with traffic having invalid destinations.

Guidelines for configuring ICMP rate-limiting

Apply ICMP rate-limiting on all connected interfaces on the switch to effectively throttle excessive ICMP messaging from any source. Figure 76 (page 160) shows an example of how to configure this for a small to mid-sized campus though similar rate-limit thresholds are applicable to other network environments. On edge interfaces, where ICMP traffic should be minimal, a threshold of 1% of available bandwidth should be sufficient for most applications. On core interfaces, such as switch-to-switch and switch-to-router, a maximum threshold of 5% should be sufficient for normal ICMP traffic. ("Normal" ICMP traffic levels should be the maximums that occur when the network is rebooting.)

Figure 76 Example of ICMP rate-limiting



NOTE: When using kbps-mode ICMP rate-limiting, the rate-limiting operates on only the IP payload part of the ICMP packet (as required by metering RFC 2698). This means that effective metering is at a rate greater than the configured rate, with the disparity increasing as the packet size decreases (the packet to payload ratio is higher).

Also, in kbps mode, metering accuracy is limited at low values, for example, less than 45 Kbps. This is to allow metering to function well at higher media speeds such as 10 Gbps.

Using both ICMP rate-limiting and all-traffic rate-limiting on the same interface

ICMP and all-traffic rate-limiting can be configured on the same interface. All-traffic rate-limiting applies to all inbound or outbound traffic (including ICMP traffic), while ICMP rate-limiting applies only to inbound ICMP traffic.

NOTE: If the all-traffic load on an interface meets or exceeds the currently configured all-traffic inbound rate-limit while the ICMP traffic rate-limit on the same interface has not been reached, all excess traffic is dropped, including any inbound ICMP traffic above the all-traffic limit (regardless of whether the ICMP rate-limit has been reached).

Example

Suppose:

- The all-traffic inbound rate-limit on port "X" is configured at 55% of the port's bandwidth.
- The ICMP traffic rate-limit on port "X" is configured at 2% of the port's bandwidth.

If at a given moment:

- Inbound ICMP traffic on port "X" is using 1% of the port's bandwidth, and
- Inbound traffic of all types on port "X" demands 61% of the ports's bandwidth,

all inbound traffic above 55% of the port's bandwidth, including any additional ICMP traffic, is dropped as long as all inbound traffic combined on the port demands 55% or more of the port's bandwidth.

Operating notes for ICMP rate-limiting

ICMP rate-limiting operates on an interface (per-port) basis to allow, on average, the highest expected amount of legitimate, inbound ICMP traffic.

- **Interface support:** ICMP rate-limiting is available on all types of ports (other than trunk ports or mesh ports), and at all port speeds configurable for the switch.
- **Rate-limiting is not permitted on mesh ports:** Either type of rate-limiting (all-traffic or ICMP) can reduce the efficiency of paths through a mesh domain.
- **Rate-limiting is not supported on port trunks:** Neither all-traffic nor ICMP rate-limiting are supported on ports configured in a trunk group.
- **ICMP percentage-based rate-limits are calculated as a percentage of the negotiated link speed:** For example, if a 100 Mbps port negotiates a link to another switch at 100 Mbps and is ICMP rate-limit configured at 5%, the inbound ICMP traffic flow through that port is limited to 5 Mbps. Similarly, if the same port negotiates a 10 Mbps link, it allows 0.5 Mbps of inbound traffic. If an interface experiences an inbound flow of ICMP traffic in excess of its configured limit, the switch generates a log message and an SNMP trap (if an SNMP trap receiver is configured).
- **ICMP rate-limiting is port-based:** ICMP rate-limiting reflects the available percentage of an interface's entire inbound bandwidth. The rate of inbound flow for traffic of a given priority and the rate of flow from an ICMP rate-limited interface to a particular queue of an outbound interface are not measures of the actual ICMP rate limit enforced on an interface.
- **Below-maximum rates:** ICMP rate-limiting operates on a per-interface basis, regardless of traffic priority. Configuring ICMP rate-limiting on an interface where other features affect inbound port queue behavior (such as flow control) can result in the interface not achieving its configured ICMP rate-limiting maximum. For example, in some situations with flow control configured on an ICMP rate-limited interface, there can be enough "back pressure" to hold high-priority inbound traffic from the upstream device or application to a rate that does not allow bandwidth for lower-priority ICMP traffic. In this case, the inbound traffic flow may not permit the forwarding of ICMP traffic into the switch fabric from the rate-limited interface. (This behavior is termed "head-of-line blocking" and is a well-known problem with flow-control.) In cases where both types of rate-limiting (`rate-limit all` and `rate-limit icmp`) are configured on the same interface, this situation is more likely to occur.

  In another type of situation, an outbound interface can become oversubscribed by traffic received from multiple ICMP rate-limited interfaces. In this case, the actual rate for traffic on the rate-limited interfaces may be lower than configured because the total traffic load requested to the outbound interface exceeds the interface's bandwidth, and thus some requested traffic may be held off on inbound.
- **Monitoring (mirroring) ICMP rate-limited interfaces:** If monitoring is configured, packets dropped by ICMP rate-limiting on a monitored interface are still forwarded to the designated monitor port. (Monitoring shows what traffic is inbound on an interface, and is not affected by "drop" or "forward" decisions.)

- **Optimum rate-limiting operation:** Optimum rate-limiting occurs with 64-byte packet sizes. Traffic with larger packet sizes can result in performance somewhat below the configured inbound bandwidth. This is to ensure the strictest possible rate-limiting of all sizes of packets.
- **Outbound traffic flow:** Configuring ICMP rate-limiting on an interface does *not* control the rate of outbound traffic flow on the interface.

Notes on testing ICMP rate-limiting

ICMP rate-limiting is applied to the available bandwidth on an interface. If the total bandwidth requested by all ICMP traffic is less than the available, configured maximum rate, no ICMP rate-limit can be applied. That is, an interface must be receiving more inbound ICMP traffic than the configured bandwidth limit allows. If the interface is configured with both `rate-limit all` and `rate-limit icmp`, the ICMP limit can be met or exceeded only if the rate limit for all types of inbound traffic has not already been met or exceeded. Also, to test the ICMP limit you need to generate ICMP traffic that exceeds the configured ICMP rate limit. Using the recommended settings—1% for edge interfaces and 5% maximum for core interfaces—it is easy to generate sufficient traffic. However, if you are testing with higher maximums, you need to ensure that the ICMP traffic volume exceeds the configured maximum.

When testing ICMP rate-limiting where inbound ICMP traffic on a given interface has destinations on multiple outbound interfaces, the test results must be based on the received outbound ICMP traffic.

ICMP rate-limiting is not reflected in counters monitoring inbound traffic because inbound packets are counted before the ICMP rate-limiting drop action occurs.

ICMP rate-limiting trap and Event Log messages

If the switch detects a volume of inbound ICMP traffic on a port that exceeds the ICMP rate-limit configured for that port, it generates one SNMP trap and one informational Event Log message to notify the system operator of the condition. (The trap and Event Log message are sent within two minutes of when the event occurred on the port.) For example:

```
I 06/30/05 11:15:42 RateLim: ICMP traffic exceeded configured limit on
port A1
```

These trap and Event Log messages provide an advisory that inbound ICMP traffic on a given interface has exceeded the configured maximum. The additional ICMP traffic is dropped, but the excess condition may indicate an infected host (or other traffic threat or network problem) on that interface. The system operator should investigate the attached devices or network conditions further; the switch does not send more traps or Event Log messages for excess ICMP traffic on the affected port until the system operator resets the port's ICMP trap function.

The switch does not send more traps or Event Log messages for excess ICMP traffic on the affected port until the system operator resets the port’s ICMP trap function. The reset can be done through SNMP from a network management station or through the CLI with the `trap-clear` command option or the `setmib` command.

Guaranteed minimum bandwidth (GMB)

GMB provides a method for ensuring that each of a given port's outbound traffic priority queues has a specified minimum consideration for sending traffic out on the link to another device. This can prevent a condition where applications generating lower-priority traffic in the network are frequently or continually "starved" by high volumes of higher-priority traffic. You can configure GMB per-port.

Terminology

Oversubscribed Queue: The condition where there is insufficient bandwidth allocated to a particular outbound priority queue for a given port. If additional, unused bandwidth is not available, the port delays or drops the excess traffic.

GMB operation

The switch services per-port outbound traffic in a descending order of priority; that is, from the highest priority to the lowest priority. By default, each port offers eight prioritized, outbound traffic queues. Tagged VLAN traffic is prioritized according to the 802.1p priority the traffic carries. Untagged VLAN traffic is assigned a priority of **0** (normal).

Table 20 Per-port outbound priority queues

802.1p Priority settings in tagged VLAN packets[1]	Outbound priority queue for a given port
1 (low)	1
2 (low)	2
0 (normal)	3
3 (normal)	4
4 (medium)	5
5 (medium)	6
6 (high)	7
7 (high)	8

[1] The switch processes outbound traffic from an untagged port at the "0" (normal) priority level.

You can use GMB to reserve a specific percentage of each port's available outbound bandwidth for each of the eight priority queues. This means that regardless of the amount of high-priority outbound traffic on a port, you can ensure that there will always be bandwidth reserved for lower-priority traffic.

Since the switch services outbound traffic according to priority (highest to lowest), the highest-priority outbound traffic on a given port automatically receives the first priority in servicing. Thus, in most applications, it is necessary only to specify the minimum bandwidth you want to allocate to the lower priority queues. In this case, the high-priority traffic automatically receives all unassigned bandwidth without starving the lower-priority queues.

Conversely, configuring a bandwidth minimum on only the high-priority outbound queue of a port (and not providing a bandwidth minimum for the lower-priority queues) is not recommended, because it may "starve" the lower-priority queues. (See the 163.)

NOTE: For a given port, when the demand on one or more outbound queues exceeds the minimum bandwidth configured for those queues, the switch apportions unallocated bandwidth to these queues on a priority basis. As a result, specifying a minimum bandwidth for a high-priority queue but not specifying a minimum for lower-priority queues can starve the lower-priority queues during periods of high demand on the high priority queue. For example, if a port configured to allocate a minimum bandwidth of 80% for outbound high-priority traffic experiences a demand above this minimum, this burst starves lower-priority queues that *do not have a minimum configured*. Normally, this will not altogether halt lower priority traffic on the network, but will likely cause delays in the delivery of the lower-priority traffic.

The sum of the GMB settings for all outbound queues on a given port cannot exceed 100%.

Impacts of QoS queue configuration on GMB operation

The section on “Configuring Guaranteed Minimum Bandwidth (GMB) for outbound traffic” (page 149) assumes the ports on the switch offer eight prioritized, outbound traffic queues. This may not always be the case, however, because the switch supports aQoS queue configuration feature that allows you to reduce the number of outbound queues from eight (the default) to four queues, or two.

Changing the number of queues affects the GMB commands (`interface bandwidth-min` and `show bandwidth output`) such that they operate only on the number of queues currently configured. If the queues are reconfigured, the guaranteed minimum bandwidth per queue is automatically re-allocated according to the following percentages:

Table 21 Default GMB percentage allocations per QoS queue configuration

802.1p priority	8 queues (default)	4 queues	2 queues
1 (lowest)	2%	10%	90%
2	3%		
0 (normal)	30%	70%	
3	10%		
4	10%	10%	10%
5	10%		
6	15%	10%	
7 (highest)	20%		

NOTE: For more information on queue configuration and the associated default minimum bandwidth settings, see chapter "*Quality of Service (QoS): Managing Bandwidth More Effectively*" in the *Advanced Traffic Management Guide* for your switch.

Impact of QoS queue configuration on GMB commands.

Changing the number of queues causes the GMB commands (`interface bandwidth-min` and `show bandwidth output`) to operate only on the number of queues currently configured. In addition, when the `qos queue-config` command is executed, any previously configured `bandwidth-min output` settings are removed from the startup configuration. For the default GMB percentage allocations per number of queues, see “Default GMB percentage allocations per QoS queue configuration” (page 164).

Jumbo frames

The maximum transmission unit(MTU) is the maximum size IP frame the switch can receive for Layer 2 frames inbound on a port. The switch drops any inbound frames larger than the MTU allowed on the port. Ports operating at a minimum of 10 Mbps on the HP 3500 switches and 1 Gbps on the other switches covered in this guide can accept forward frames of up to 9220 bytes (including four bytes for a VLAN tag) when configured for jumbo traffic. You can enable inbound jumbo frames on a per-VLAN basis. That is, on a VLAN configured for jumbo traffic, all ports belonging to that VLAN and *operating* at a minimum of 10 Mbps on the HP 3500 switches and 1 Gbps on the other switches covered in this guide allow inbound jumbo frames of up to 9220 bytes.

Switch model	Minimum speed for jumbo traffic
3500	10 Mbps
All others in this guide	1 Gbps

Terminology

Term	Definition
Jumbo Frame	An IP frame exceeding 1522 bytes. The maximum jumbo frame size is 9220 bytes. (This size includes 4 bytes for the VLAN tag.)
Jumbo VLAN	A VLAN configured to allow inbound jumbo traffic. All ports belonging to a jumbo and operating at 1 Gbps or higher can receive jumbo frames from external devices. If the switch is in a meshed domain, all meshed ports (operating at 1 Gbps or higher) on the switch accept jumbo traffic from other devices in the mesh.
MTU (Maximum Transmission Unit)	This is the maximum-size IP frame the switch can receive for Layer 2 frames inbound on a port. The switch allows jumbo frames of up to 9220 bytes.
Standard MTU	An IP frame of 1522 bytes. (This size includes 4 bytes for the VLAN tag.)

Operating rules

- **Required port speed**: This feature allows inbound and outbound jumbo frames on ports operating at a minimum of 10 Mbps on the HP 3500 switches and 1 Gbps on the other switches.
- **Switch meshing**: If you enable jumbo traffic on a VLAN, all meshed ports on the switch are enabled to support jumbo traffic. (On a given meshed switch, every meshed port operating at 1 Gbps or higher becomes a member of every VLAN configured on the switch.)
- **GVRP operation**: A VLAN enabled for jumbo traffic cannot be used to create a dynamic VLAN. A port belonging to a statically configured, jumbo-enabled VLAN cannot join a dynamic VLAN.
- **Port adds and moves**: If you add a port to a VLAN that is already configured for jumbo traffic, the switch enables that port to receive jumbo traffic. If you remove a port from a jumbo-enabled VLAN, the switch disables jumbo traffic capability on the port only if the port is not currently a member of another jumbo-enabled VLAN. This same operation applies to port trunks.
- **Jumbo traffic sources**: A port belonging to a jumbo-enabled VLAN can receive inbound jumbo frames through any VLAN to which it belongs, including non-jumbo VLANs. For example, if VLAN 10 (without jumbos enabled) and VLAN 20 (with jumbos enabled) are both configured on a switch, and port 1 belongs to both VLANs, port 1 can receive jumbo traffic from devices on either VLAN. For a method to allow only some ports in a VLAN to receive jumbo traffic, see "Configuring a maximum frame size" (page 155).

SNMP implementation

Jumbo maximum frame size

The maximum frame size for jumbos is supported with the following proprietary MIB object:

```
hpSwitchMaxFrameSize OBJECT-TYPE
```

This is the value of the global `max-frame-size` supported by the switch. The default value is set to 9216 bytes.

Jumbo IP MTU

The IP MTU for jumbos is supported with the following proprietary MIB object:

```
hpSwitchIpMTU OBJECT-TYPE
```

This is the value of the global jumbos IP MTU (or L3 MTU) supported by the switch. The default value is set to 9198 bytes (a value that is 18 bytes less than the largest possible maximum frame size of 9216 bytes). This object can be used only in switches that support `max-frame-size` and `ip-mtu` configuration.

Operating notes for jumbo traffic-handling

- HP Switch does not recommend configuring avoice VLAN to accept jumbo frames. Voice VLAN frames are typically small, and allowing a voice VLAN to accept jumbo frame traffic can degrade the voice transmission performance.
- You can configure the default, primary, and/or (if configured) the management VLAN to accept jumbo frames on all ports belonging to the VLAN.
- When the switch applies the default MTU (1522-bytes including 4 bytes for the VLAN tag) to a VLAN, all ports in the VLAN can receive incoming frames of up to 1522 bytes. When the switch applies the jumbo MTU (9220 bytes including 4 bytes for the VLAN tag) to a VLAN, all ports in that VLAN can receive incoming frames of up to 9220 bytes. A port receiving frames exceeding the applicable MTU drops such frames, causing the switch to generate an Event Log message and increment the "Giant Rx" counter (displayed by `show interfaces port-list`).
- The switch allows flow control and jumbo frame capability to co-exist on a port.
- The default MTU is 1522 bytes (including 4 bytes for the VLAN tag). The jumbo MTU is 9220 bytes (including 4 bytes for the VLAN tag).
- When a port is not a member of any jumbo-enabled VLAN, it drops all jumbo traffic. If the port is receiving "excessive"inbound jumbo traffic, the port generates an Event Log message to notify you of this condition. This same condition also increments the switch's "Giant Rx" counter.
- If you do not want all ports in a given VLAN to accept jumbo frames, you can consider creating one or more jumbo VLANs with a membership comprising only the ports you want to receive jumbo traffic. Because a port belonging to one jumbo-enabled VLAN can receive jumbo frames through any VLAN to which it belongs, this method enables you to include both jumbo-enabled and non-jumbo ports within the same VLAN.

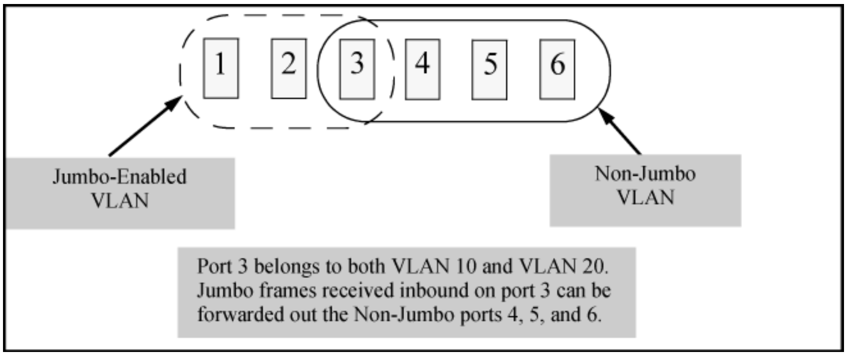
  For example, suppose you want to allow inbound jumbo frames only on ports 6, 7, 12, and 13. However, these ports are spread across VLAN 100 and VLAN 200 and also share these VLANs with other ports you want excluded from jumbo traffic. A solution is to create a third VLAN with the sole purpose of enabling jumbo traffic on the desired ports, while leaving the other ports on the switch disabled for jumbo traffic. That is:

	VLAN 100	VLAN 200	VLAN 300
Ports	6-10	11-15	6, 7, 12, and 13
Jumbo-enabled?	No	No	Yes

  If there are security concerns with grouping the ports as shown for VLAN 300, you can either use source-port filtering to block unwanted traffic paths or create separate jumbo VLANs, one for ports 6 and 7, and another for ports 12 and 13.

- **Outbound jumbo traffic.** Any port operating at 1 Gbps or higher can transmit outbound jumbo frames through any VLAN, regardless of the jumbo configuration. The VLAN is not required to be jumbo-enabled, and the port is not required to belong to any other, jumbo-enabled VLANs. This can occur in situations where a non-jumbo VLAN includes some ports that do not belong to another, jumbo-enabled VLAN and some ports that do belong to another, jumbo-enabled VLAN. In this case, ports capable of receiving jumbo frames can forward them to the ports in the VLAN that do not have jumbo capability, as shown in Figure 77.

Figure 77 Forwarding jumbo frames through non-jumbo ports


1
2
3
4
5
6
Jumbo-Enabled VLAN
Non-Jumbo VLAN
Port 3 belongs to both VLAN 10 and VLAN 20. Jumbo frames received inbound on port 3 can be forwarded out the Non-Jumbo ports 4, 5, and 6.

Jumbo frames can also be forwarded out non-jumbo ports when the jumbo frames received inbound on a jumbo-enabled VLAN are routed to another, non-jumbo VLAN for outbound transmission on ports that have no memberships in other, jumbo-capable VLANs. Where either of the above scenarios is a possibility, the downstream device must be configured to accept the jumbo traffic. Otherwise, this traffic will be dropped by the downstream device.

- **Jumbo traffic in a switch mesh domain.** If a switch belongs to a meshed domain, but does not have any VLANs configured to support jumbo traffic, the meshed ports on that switch drop any jumbo frames they receive from other devices. In this regard, if a mesh domain includes any HP 1600M/2400M/2424M/4000M/8000M switches, along with the switches covered in this guide configured to support jumbo traffic, only the switches covered in this guide receive jumbo frames. The other switch models in the mesh will drop such frames. For more information on switch meshing, see chapter "Switch Meshing" in the *Advanced Traffic Management Guide* for your switch.

Troubleshooting

A VLAN is configured to allow jumbo frames, but one or more ports drops all inbound jumbo frames

The port may not be operating at a minimum of 10 Mbps on the HP 3500 switches or 1 Gbps on the other switches covered in this guide. Regardless of a port's configuration, if it is actually operating at a speed lower than 10 Mbps for HP 3500 switches or 1 Gbps for the other switches, it drops inbound jumbo frames. For example, if a port is configured for `Auto` mode (`speed-duplex auto`), but has negotiated a 7 Mbps speed with the device at the other end of the link, the port cannot receive inbound jumbo frames. To determine the actual operating speed of one or more ports, view the `Mode` field in the output for the following command:

```
show interfaces brief port-list
```

A non-jumbo port is generating "Excessive undersize/giant frames" messages in the Event Log

The switches can transmit outbound jumbo traffic on any port, regardless of whether the port belongs to a jumbo VLAN. In this case, another port in the same VLAN on the switch may be jumbo-enabled through membership in a different, jumbo-enabled VLAN, and may be forwarding jumbo frames received on the jumbo VLAN to non-jumbo ports.

7 Configuring for Network Management Applications

Command Summary

Table 22 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
[no] snmpv3 user *user_name*	Adds or deletes a user entry for SNMPv3.	-	(page 172)	-
[auth | md5 | sha *auth_pass*]	With authorization, you can set either MD5 or SHA authentication.	None	(page 172)	-
[priv | des | aes *priv_pass*]	With privacy, the switch supports DES (56-bit) and AES (128-bit) encryption.	DES	(page 172)	-
show snmpv3 user	Displays information about the management stations configured on VLAN 1 to access the switch.	-	(page 174)	-
[no] snmpv3 group	Assigns or removes a user to a security group for access rights to the switch.	-	(page 174)	-
[no] snmpv3 community	Maps or removes a mapping of a community name to a group access level.	-	(page 175)	(page 177)
show snmp-server [community-string]	Lists the data for currently configured SNMP community names.	-	(page 176)	-
[no] snmp-server community *community-name*	Configures a new community name.	-	(page 176)	(page 177)
snmp-server host *ipv4-addr* | *ipv6-addr* *community name*	Configures a destination network management station to receive SNMPv1/v2c traps and (optionally) Event Log messages sent as traps from the switch	Public	(page 178)	-
[no] snmp-server host [*ipv4-addr* | *ipv6-addr*] *community name* inform [retries *count*][timeout *interval*]	Enables (or disables) the inform option for SNMPv2c on the switch and allows you to configure options for sending SNMP inform requests.	-	(page 179)	-
[no] snmpv3 notify *notify_name* tagvalue *tag_name*	Associates the name of an SNMPv3 notification configuration with a tag name used (internally) in SNMPv3 commands.	-	(page 180)	-
[no] snmpv3 targetaddress [*ipv4-addr* | *ipv6-addr*] *name*	Configures the IPv4 or IPv6 address, name, and configuration filename of the SNMPv3 management station to which notification messages are sent.	-	(page 180)	-
[no] snmpv3 params *params_name* user *user_name*	Applies the configuration parameters and IP address of an SNMPv3 management	-	(page 180)	-

Table 22 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
	station to a specified SNMPv3 user			
[no] snmp-server enable traps [snmp-auth | password-change-mgr | login-failure-mgr | port-security | auth-server-fail | dhcp-snooping | arp-protect | running-config-change]	Enables or disables sending one of the security notification types listed below to configured trap receivers.	Enabled	(page 182)	-
[no] snmp-server enable traps link-change *port-list* [all]	Enables or disables the switch to send a link-change trap to configured trap receivers when the link state on a port goes from up to down or down to up.	-	(page 184)	-
[no] snmp-server enable traps running-config-change [transmission-interval 0-4294967295]	Enables SNMP traps being sent when changes to the running configuration file are made.	Disabled	(page 184)	-
show running-config [changes-history [1-32]][detail]	Displays the history up to 32 events for changes made to the running-configuration file.	-	(page 185)	-
[no] snmp-server response-source [dst-ip-of-request | *ipv4-addr* | *ipv6-addr* | loopback0-7]	Specifies the source IP address of the SNMP response PDU.	Interface IP address	(page 187)	-
[no] snmp-server trap-source [*ipv4-addr* | loopback0-7]	Specifies the source IP address to be used for a trap PDU.	The interface IP address in generated trap PDUs	(page 187)	-
show snmp-server	Displays the SNMP policy configuration and the currently configured notification settings for versions SNMPv1 and SNMPv2c traps.	-	(page 187) and (page 188)	-
snmp-server [listen [oobm | data | both]]	Enables or disables inbound SNMP access on a switch.	Both	(page 193)	-
[no] sflow *receiver-instance* destination *ip-address* [udp-port-num]	Enables an sFlow receiver/destination.	-	(page 193)	-
sflow *receiver-instance* sampling *port-list* *sampling rate*	Once an sFlow receiver/destination has been enabled, this command enables flow sampling for that instance.	-	(page 193)	-
sflow *receiver-instance* polling *port-list* *polling interval*	Once an sFlow receiver/destination has been enabled, this command enables counter polling for that instance.	-	(page 193)	-
show sflow agent	Displays sFlow agent information.	-	(page 194)	-

Table 22 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`show sflow` *`receiver instance`* `destination`	Displays information about the management station to which the sFlow sampling-polling data is sent.	-	(page 194)	-
`show sflow` *`receiver instance`* `sampling-polling port-list/range`	Displays status information about sFlow sampling and polling.	-	(page 194)	-
`show lldp config`	Displays the LLDP global configuration, LLDP port status, and SNMP notification status.	-	(page 195)	-
`show lldp config` *`port-list`*	Displays the LLDP port-specific configuration for all ports in *`port-list`* .	-	(page 196)	-
`[no] lldp run`	Enables or disables LLDP operation on the switch.	Enabled	(page 196)	-
`lldp refresh-interval 5 - 32768`	Changes the interval between consecutive transmissions of LLDP advertisements on any given port.	30 seconds	(page 197)	-
`lldp holdtime-multiplier 2 - 10`	Changes the multiplier an LLDP switch uses to calculate the Time-to-Live for the LLDP advertisements it generates and transmits to LLDP neighbors.	4	(page 197)	-
`setmib lldpTxDelay.0 -i 1 - 8192`	Uses `setmib` to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements because of a change in LLDP MIB content	2	(page 197)	-
`setmib lldpReinitDelay.0 -i 1 - 10`	Uses `setmib` to change the minimum time (reinitialization delay interval) an LLDP port will wait before reinitializing after receiving an LLDP disable command followed closely by a txonly or tx_rx command.	2 seconds	(page 198)	-
`[no] lldp enable-notification` *`port-list`*	Enables or disables each port in *`port-list`* for sending notification to configured SNMP trap receivers if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor.	Disabled	(page 198)	-
`setmib lldpnotificationinterval.0 -i 1 - 3600`	Globally changes the interval between successive traps generated by the switch.	5 seconds	(page 199)	-
`lldp admin-status` *`port-list`* `[ txonly | rxonly | tx_rx | disable ]`	Options for controlling which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.	tx_rx	(page 199)	-

Table 22 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
[no] lldp config *port-list* ipAddrEnable *ip-address*	Replaces the default IP address for the port with an IP address you specify.	-	(page 200)	-
[no] lldp config *port-list* basicTlvEnable *TLV-Type*	Configures an individual port or group of ports to exclude one or more data types from outbound LLDP advertisements.	-	(page 200)	-
[no] lldp config *port-list* dot3TlvEnable macphy_config	For outbound advertisements, this TLV includes the (local) switch port's current speed and duplex settings, the range of speed and duplex settings the port supports, and the method required for reconfiguring the speed and duplex settings on the device.	Enabled	(page 201)	-
[no] lldp config *port-list* dot1TlvEnable port-vlan-id	Enables the VLAN ID TLV advertisement.	Enabled	(page 201)	-
lldp top-change-notify *port-list*	Provides information an SNMP application can use to track LLDP-MED connects and disconnects.	Disabled	(page 203)	-
lldp fast-start-count 1 - 10	Temporarily overrides the `refresh-interval` setting for the `fast-start-count` advertisement interval, resulting in the port initially advertising LLDP-MED at a faster rate for a limited time.	5 seconds	(page 203)	-
[no] lldp config *port-list* medTlvEnable *medTlv*	Enables or disables advertisement of specified TLVs on the specified ports, helps to locate configuration mismatches, and so on.	-	(page 204)	-
[no] lldp config *port-list* medPortLocation *Address-Type*	Configures location of emergency call data the switch advertises per port in the `location_id` TLV	-	(page 205)	-
show lldp info local-device [*port-list*]	Displays the current switch information that will be used to populate outbound LLDP advertisements.	-	(page 208)	-
show interfaces brief *port-list*	Includes port speed and duplex configuration in the `Mode` column of the resulting display.	-	(page 209)	-
show lldp info remote-device [*port-list*]	Displays the content of the inbound LLDP advertisements received from other LLDP devices.	-	(page 209)	-
show lldp stats [*port-list*]	Displays LLDP statistics on both global and per-port levels.	-	(page 210)	-

Table 22 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`show cdp`	Lists the global and per-port CDP configuration of the switch.	-	(page 212)	-
`show cdp neighbors`	Lists the neighboring CDP devices the switch detects.	-	(page 213)	-
`[no] cdp run`	Enables or disables CDP read-only operation on the switch.	Enabled	(page 214)	-
`[no] cdp enable [ [ e ] port-list ]`	Disabling CDP on a port causes it to drop inbound CDP packets without recording their data in the CDP Neighbors table.	Enabled	(page 214)	-

For overview information on using SNMPv3, see "About using SNMP tools to manage the switch" (page 217).

For information on enabling SNMPv3, see "SNMPv3 users" (page 219).

Enabling SNMPv3

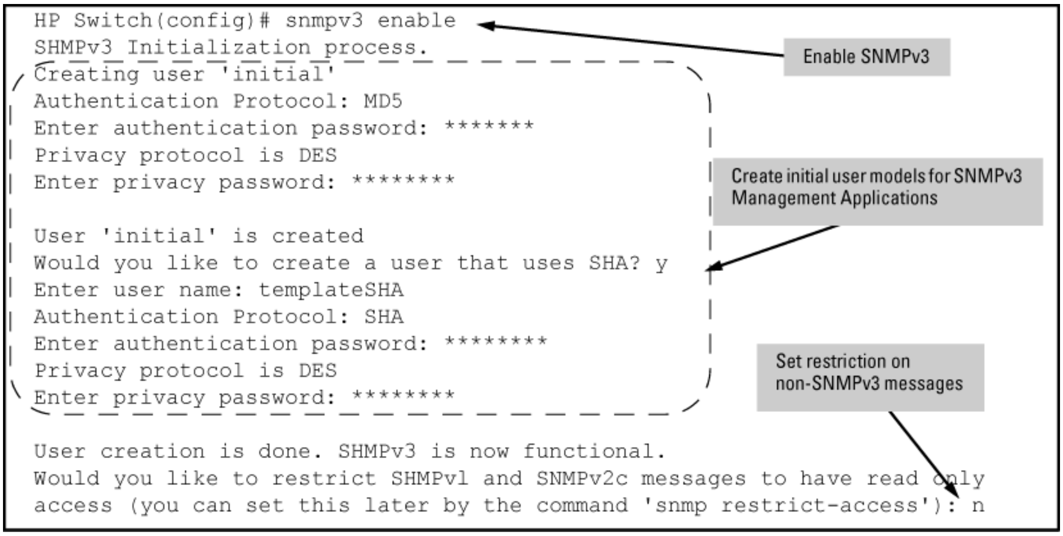
The `snmpv3 enable` command allows the switch to:

- Receive SNMPv3 messages.
- Configure initial users.
- Restrict non-version 3 messages to "read only" (optional).

△ **CAUTION:** Restricting access to only version 3 messages makes the community named "public" inaccessible to network management applications (such as autodiscovery, traffic monitoring, SNMP trap generation, and threshold setting) from operating in the switch.

Example

Example 42 SNMP version 3 `enable` command



```
HP Switch(config)# snmpv3 enable
SHMPv3 Initialization process.
Creating user 'initial'
Authentication Protocol: MD5
Enter authentication password: *******
Privacy protocol is DES
Enter privacy password: ********

User 'initial' is created
Would you like to create a user that uses SHA? y
Enter user name: templateSHA
Authentication Protocol: SHA
Enter authentication password: ********
Privacy protocol is DES
Enter privacy password: ********

User creation is done. SHMPv3 is now functional.
Would you like to restrict SHMPvl and SNMPv2c messages to have read only
access (you can set this later by the command 'snmp restrict-access'): n
```

Enable SNMPv3
Create initial user models for SNMPv3 Management Applications
Set restriction on non-SNMPv3 messages

Configuring users (CLI)

For information on users, see "SNMPv3 users" (page 219).

Syntax:

`[no] snmpv3 user` *`user_name`*

Adds or deletes a user entry for SNMPv3. Authorization and privacy are optional, but to use privacy, you must use authorization. When you delete a user, only the *`user_name`* is required.

`[ auth  md5 | sha` *`auth_pass`* `]`

With authorization, you can set either MD5 or SHA authentication. The authentication password *`auth_pass`* must be 6 to 32 characters and is mandatory when you configure authentication.

(Default: None)

`[ priv  des | aes` *`priv_pass`* `]`

With privacy, the switch supports DES (56-bit) and AES (128-bit) encryption. The privacy password *`priv_pass`* must be 6 to 32 characters and is mandatory when you configure privacy.

(Default: DES)

NOTE: Only AES 128-bit and DES 56-bit encryption are supported as privacy protocols. Other non-standard encryption algorithms, such as AES-172, AES-256, and 3-DES are not supported.

NOTE: For the 5400zl, 3800, and 8200zl switches, when the switch is in enhanced secure mode, commands that take a password as a parameter have the echo of the password typing replaced with asterisks. The input for the password is prompted for interactively. Additionally, the DES option is not available. For more information, see the chapter "Secure Mode (5400zl, 3800, and 8200zl Switches)" in the Access Security Guide for your switch.

Enabling and disabling switch for access from SNMPv3 agents

This includes the creation of the initial user record.

Syntax:

```
[no] snmpv3 enable
```

Enabling or disabling restrictions to access from only SNMPv3 agents

When enabled, the switch rejects all non-SNMPv3 messages.

Syntax:

```
[no] snmpv3 only
```

Enabling or disabling restrictions from all non-SNMPv3 agents to read-only access

Syntax:

```
[no] snmpv3 restricted-access
```

Viewing the operating status of SNMPv3

Syntax:

```
show snmpv3 enable
```

Viewing status of message reception of non-SNMPv3 messages

Syntax:

```
show snmpv3 only
```

Viewing status of write messages of non-SNMPv3 messages

Syntax:

```
show snmpv3 restricted-access
```

Viewing management stations configured to access the switch and view authentication and privacy protocols of each station (CLI)

Syntax:

```
show snmpv3 user
```

Example

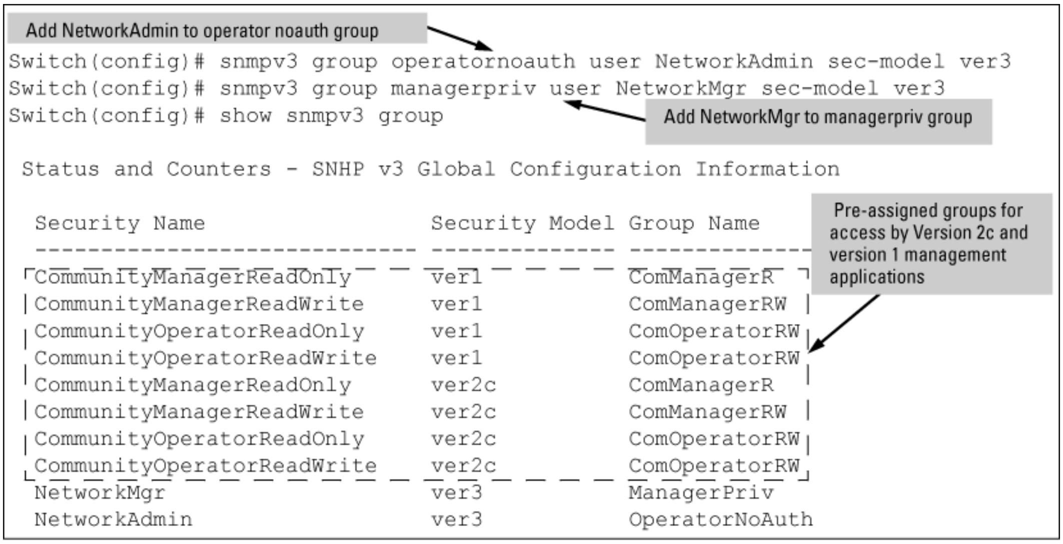
Example 43 Displays information about the management stations configured on VLAN 1 to access the switch

```
HP Switch# configure terminal
HP Switch(config)# vlan 1
HP Switch(vlan-1)# show snmpv3 user

Status and Counters - SNMPv3 Global Configuration Information

 User Name      Auth. Protocol   Privacy Protocol
 -----------    --------------   -----------------
 initial        MD5              CFB AES-128
 NetworkAdmin   MD5              CBC-DES
```

Assigning users to groups (CLI)

Next you must set the group access level for the user by assigning the user to a group. This is done with the `snmpv3 group` command, as shown in Figure 78 (page 174). For more details on the MIBs access for a given group, see "Group access levels" (page 220).

Figure 78 Example of assigning users to groups



Add NetworkAdmin to operator noauth group

```
Switch(config)# snmpv3 group operatornoauth user NetworkAdmin sec-model ver3
Switch(config)# snmpv3 group managerpriv user NetworkMgr sec-model ver3
Switch(config)# show snmpv3 group

 Status and Counters - SNHP v3 Global Configuration Information

  Security Name                  Security Model Group Name
  ------------------------------ -------------- -------------
  CommunityManagerReadOnly       ver1           ComManagerR
  CommunityManagerReadWrite      ver1           ComManagerRW
  CommunityOperatorReadOnly      ver1           ComOperatorRW
  CommunityOperatorReadWrite     ver1           ComOperatorRW
  CommunityManagerReadOnly       ver2c          ComManagerR
  CommunityManagerReadWrite      ver2c          ComManagerRW
  CommunityOperatorReadOnly      ver2c          ComOperatorRW
  CommunityOperatorReadWrite     ver2c          ComOperatorRW
  NetworkMgr                     ver3           ManagerPriv
  NetworkAdmin                   ver3           OperatorNoAuth
```

Add NetworkMgr to managerpriv group

Pre-assigned groups for access by Version 2c and version 1 management applications

Syntax:

```
[no] snmpv3 group
```

Assigns or removes a user to a security group for access rights to the switch. To delete an entry, all of the following three parameters must be included in the command:

`group group_name`	Identifies the group that has the privileges that will be assigned to the user. For more details, see "Group access levels" (page 220).
`user user_name`	Identifies the user to be added to the access group. This must match the user name added with the `snmpv3 user` command.
`sec-model[ ver1 | ver2c | ver3 ]`	Defines which security model to use for the added user. An SNMPv3 access group should use only the ver3 security model.

Mapping SNMPv3 communities (CLI)

SNMP commuities are supported by the switch to allow management applications that use version 2c or version 1 to access the switch. For more details, see "SNMPv3 communities" (page 221).

Syntax:

```
[no] snmpv3 community
```

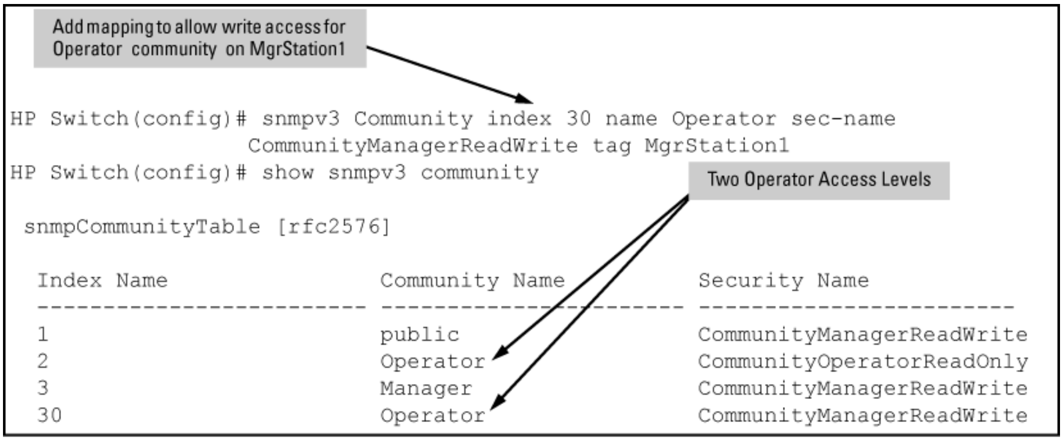
Maps or removes a mapping of a community name to a group access level. To remove a mapping you need to specify only the `index_name` parameter.

`index` *`index_name`*	An index number or title for the mapping. The values of 1 to 5 are reserved and can not be mapped.
`name` *`community_name`*	The community name that is being mapped to a group access level.
`sec-name` *`security_name`*	The group level to which the community is being mapped.
`tag` *`tag_value`*	This is used to specify which target address may have access by way of this index reference.

Example

Figure 79 (page 175) shows the assigning of the Operator community on MgrStation1 to the CommunityOperatorReadWrite group. Any other Operator has an access level of CommunityOperatorReadOnly.

Figure 79 Assigning a community to a group access level



Add mapping to allow write access for Operator community on MgrStation1
Two Operator Access Levels

```
HP Switch(config)# snmpv3 Community index 30 name Operator sec-name
                  CommunityManagerReadWrite tag MgrStation1
HP Switch(config)# show snmpv3 community

 snmpCommunityTable [rfc2576]

  Index Name                 Community Name          Security Name
  -------------------------  ----------------------- ------------------------
  1                          public                  CommunityManagerReadWrite
  2                          Operator                CommunityOperatorReadOnly
  3                          Manager                 CommunityManagerReadWrite
  30                         Operator                CommunityManagerReadWrite
```

Listing community names and values (CLI)

This command lists the data for currently configured SNMP community names (along with trap receivers and the setting for authentication traps—see "SNMP notifications" (page 221)).

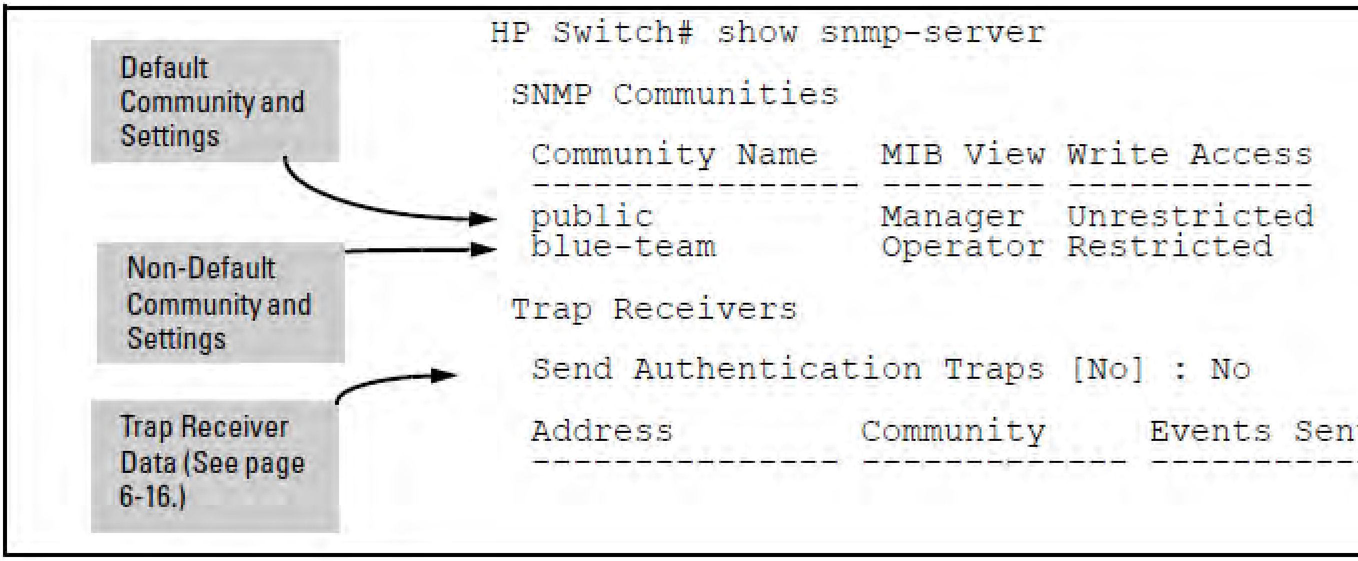
Syntax:

show snmp-server [*community-string*]

Example

Lists the data for all communities in a switch; that is, both the default "public" community name and another community named "blue-team."

Figure 80 Example of the SNMP community listing with two communities



```
HP Switch# show snmp-server

 SNMP Communities

  Community Name   MIB View Write Access
  ---------------- -------- ------------
  public           Manager  Unrestricted
  blue-team        Operator Restricted

 Trap Receivers

  Send Authentication Traps [No] : No

  Address          Community     Events Sen
  ---------------- ------------- ----------
```

Default Community and Settings
Non-Default Community and Settings
Trap Receiver Data (See page 6-16.)

To list the data for only one community, such as the "public" community, use the above command with the community name included. For example:

```
HP Switch# show snmp-server public
```

Configuring community names and values (CLI)

The `snmp-server` command enables you to add SNMP communities with either default or specific access attributes, and to delete specific communities.

Syntax:

[no] snmp-server community *community-name*

Configures a new community name.

- If you do not also specify `operator` or `manager`, the switch automatically assigns the community to the `operator` MIB view.
- If you do not specify `restricted` or `unrestricted`, the switch automatically assigns the community to `restricted` (read-only) access.

The no form uses only the *`community-name`* variable and deletes the named community from the switch.

`[ operator | manager ]`	Optionally assigns an access level. • At the `operator` level, the community can access all MIB objects except the CONFIG MIB. • At the `manager` level, the community can access all MIB objects.
`[ restricted | unrestricted ]`	Optionally assigns MIB access type. • Assigning the `restricted` type allows the community to read MIB variables, but not to set them. • Assigning the `unrestricted` type allows the community to read and set MIB variables.

Example

To add the following communities:

Community	Access Level	Type of Access
red-team	manager (*Access to all MIB objects.*)	unrestricted (*read/write*)
blue-team	operator (*Access to all MIB objects except the CONFIG MIB.*)	restricted (*read-only*)

```
HP Switch(config)# snmp-server community red-team
  manager unrestricted
HP Switch(config)# snmp-server community blue-team
  operator restricted
```

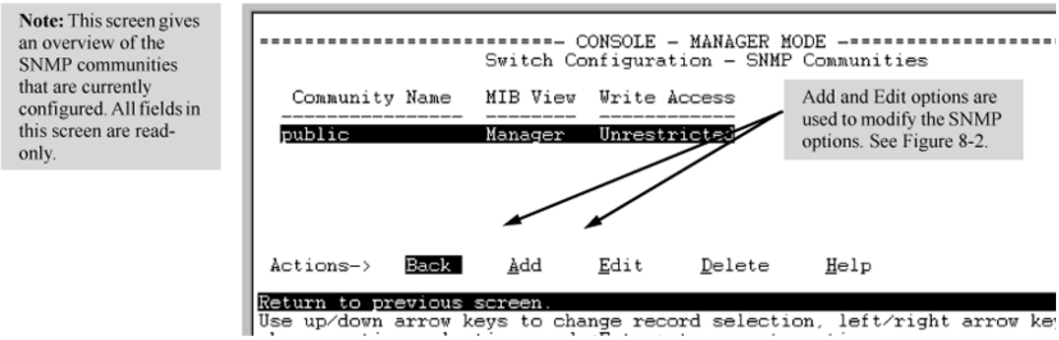
To eliminate a previously configured community named "gold-team":

```
HP Switch(config) # no snmp-server community gold-team
```

Viewing and configuring non-version-3 SNMP communities (Menu)

1. From the Main Menu, select:
   2. Switch Configuration…
   6. SNMP Community Names

Figure 81 The SNMP Communities screen (default values)



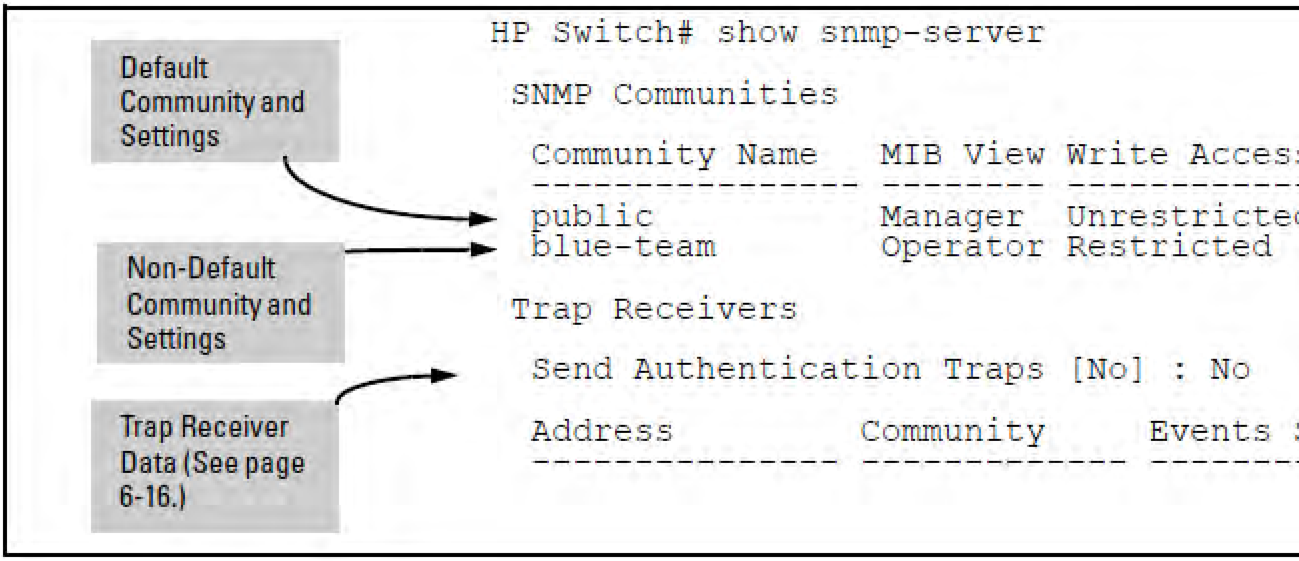
Note: This screen gives an overview of the SNMP communities that are currently configured. All fields in this screen are read-only.

```
=========================- CONSOLE - MANAGER MODE -===================
                   Switch Configuration - SNMP Communities

  Community Name   MIB View   Write Access
  --------------   --------   ------------
  public           Manager    Unrestricted



 Actions->   Back     Add     Edit     Delete     Help

Return to previous screen.
Use up/down arrow keys to change record selection, left/right arrow ke
```

Add and Edit options are used to modify the SNMP options. See Figure 8-2.

2. Press **[A]** (for **Add**) to display the following screen:

Figure 82 The SNMP add or edit screen


Default Community and Settings
Non-Default Community and Settings
Trap Receiver Data (See page 6-16.)

```
HP Switch# show snmp-server

 SNMP Communities

  Community Name    MIB View Write Acces
  ---------------- -------- -----------
  public            Manager  Unrestricte
  blue-team         Operator Restricted

 Trap Receivers

  Send Authentication Traps [No] : No

  Address          Community      Events
  ---------------- -------------- --------
```

If you need information on the options in each field, press **[Enter]** to move the cursor to the Actions line, then select the Help option. When you are finished with Help, press **[E]** (for Edit) to return the cursor to the parameter fields.

3. Enter the name you want in the Community Name field, and use the Space bar to select the appropriate value in each of the other fields. (Use the **[Tab]** key to move from one field to the next.)
4. Press **[Enter]**, then **[S]** (for **Save**).

Configuring an SNMP trap receiver (CLI)

For information about configuring SNMP trap receivers, see "SNMP trap receivers" (page 222).

Syntax:

`snmp-server host [` *`ipv4-addr`* `|` *`ipv6-addr`* `]` *`community name`*

Configures a destination network management station to receive SNMPv1/v2c traps and (optionally) Event Log messages sent as traps from the switch, using the specified community name and destination IPv4 or IPv6 address. You can specify up to ten trap receivers (network management stations). (The default community name is `public`.)

`[ none | all | not-info | critical | debug ]`	(Optional) Configures the security level of the Event Log messages you want to send as traps to a trap receiver (see Table 6-2 (page 179)). • The type of Event Log message that you specify applies only to Event Log messages, not to threshold traps. • For each configured event level, the switch continues to send threshold traps to all network management stations that have the appropriate threshold level configured. • If you do not specify an event level, the switch uses the default value (none) and sends no Event Log messages as traps.
`[inform]`	(Optional) Configures the switch to send SNMPv2 inform requests when certain events occur. For more information, see "Enabling SNMPv2c informs (CLI)" (page 179).

Table 23 Security levels for Event Log messages sent as traps

Security Level	Action
None (default)	Sends no Event Log messages.
All	Sends all Event Log messages.
Not-Info	Sends all Event Log messages that are not for information only.
Critical	Sends only Event Log messages for critical error conditions.
Debug	Sends only Event Log messages needed to troubleshoot network- and switch-level problems.

Example

To configure a trap receiver in a community named "red-team" with an IP address of 10.28.227.130 to receive only "critical" event log messages, you can enter the following command:

```
HP Switch(config)# snmp-server host 10.28.227.130 red-team critical
```

Enabling SNMPv2c informs (CLI)

For information about enabling SNMPv2c informs, see "SNMPv2c informs" (page 223).

Syntax:

`[no] snmp-server host [ *ipv4-addr* | *ipv6-addr* ]`
`*community name* inform [ retries *count* ][ timeout *interval* ]`

Enables (or disables) the `inform` option for SNMPv2c on the switch and allows you to configure options for sending SNMP inform requests.

`retries`	Maximum number of times to resend an `inform` request if no SNMP response is received. (Default: 3)
`timeout`	Number of seconds to wait for an acknowledgement before resending the `inform` request. (Default: 15 seconds)

NOTE: The `retries` and `timeout` values are not used to send trap requests.

To verify the configuration of SNMPv2c informs, enter the `show snmp-server` command, as shown in Example 44 (page 180) (note indication of inform Notify Type in bold below):

Example 44 Display of SNMPv2c inform configuration

```
HP Switch(config)# show snmp-server

 SNMP Communities

  Community Name   MIB View Write Access
  ---------------- -------- ------------ public          Manager  Unrestricted

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : All
  ...
  Address               Community       Events Sent Notify Type Retry Timeout
  --------------------- --------------- ----------- ----------- ----- --------
  15.28.333.456         guest           All         inform      3     15

 Excluded MIBs

 Snmp Response Pdu Source-IP Information

  Selection Policy   : Default rfc1517

 Trap Pdu Source-IP Information
  Selection Policy   : Configured IP
  Ip Address        : 10.10.10.10
```

Configuring SNMPv3 notifications (CLI)

The SNMPv3 notification process allows messages that are passed via SNMP between the switch and a network management station to be authenticated and encrypted.

1. Enable SNMPv3 operation on the switch by entering the `snmpv3 enable` command (See "SNMP Version 3 Commands" on page N-7).

   When SNMPv3 is enabled, the switch supports:

   - Reception of SNMPv3 notification messages (traps and informs)
   - Configuration of initial users
   - (Optional) Restriction of non-SNMPv3 messages to "read only"

2. Configure SNMPv3 users by entering the `snmpv3 user` command (see "SNMPv3 users" (page 219)). Each SNMPv3 user configuration is entered in the User Table.
3. Assign SNMPv3 users to security groups according to their level of access privilege by entering the `snmpv3 group` command (see "Assigning users to groups (CLI)" (page 174)).
4. Define the name of an SNMPv3 notification configuration by entering the `snmpv3 notify` command.

   ## Syntax:

   [no] `snmpv3 notify` *`notify_name`* `tagvalue` *`tag_name`*

   Associates the name of an SNMPv3 notification configuration with a tag name used (internally) in SNMPv3 commands. To delete a notification-to-tag mapping, enter `no snmpv3 notify` *`notify_name`*.

`notify` *`notify_name`*	Specifies the name of an SNMPv3 notification configuration.
`tagvalue` *`tag_name`*	Specifies the name of a tag value used in other SNMPv3 commands, such as `snmpv3 targetaddress params taglist` *`tag_name`* in Step 5.

5. Configure the target address of the SNMPv3 management station to which SNMPv3 informs and traps are sent by entering the `snmpv3 targetaddress` command.

Syntax:

```
[no] snmpv3 targetaddress[  ipv4-addr | ipv6-addr  ]
name
```

Configures the IPv4 or IPv6 address, name, and configuration filename of the SNMPv3 management station to which notification messages are sent.

`params` *`parms_name`*	Name of the SNMPv3 station's parameters file. The parameters filename configured with `params` *`params_name`* must match the `params` *`params_name`* value entered with the `snmpv3 params` command in Step 6.
`taglist` *`tag_name`*`[ tag_name ]` …	Specifies the SNMPv3 notifications (identified by one or more *`tag_name`* values) to be sent to the IP address of the SNMPv3 management station. You can enter more than one *`tag_name`* value. Each *`tag_name`* value must be already associated with the name of an SNMPv3 notification configuration entered with the `snmpv3 notify` command in Step 4. Use a blank space to separate *`tag_name`* values. You can enter up to 103 characters in *`tag_name`* entries following the `taglist` keyword.
`[ filter [  none | debug | all | not-info | critical ] ]`	(Optional) Configures the type of messages sent to a management station. (Default: none.)
`[ udp-port` *`port`* `]`	(Optional) Specifies the UDP port to use. (Default: 162.)
`[ port-mask` *`mask`* `]`	(Optional) Specifies a range of UDP ports. (Default: 0.)
`[ addr-mask` *`mask`* `]`	(Optional) Specifies a range of IP addresses as destinations for notification messages. (Default: 0.)
`[ retries` *`value`* `]`	(Optional) Number of times a notification is retransmitted if no response is received. Range: 1-255. (Default: 3.)
`[ timeout` *`value`* `]`	(Optional) Time (in millisecond increments) allowed to receive a response from the target before notification packets are retransmitted. Range: 0-2147483647. [Default: 1500 (15 seconds).]
`[ max-msg-size`*`size`* `]`	(Optional) Maximum number of bytes supported in a notification message to the specified target. (Default: 1472)

6. Create a configuration record for the target address with the `snmpv3 params` command.

Syntax:

```
[no] snmpv3 params params_name user user_name
```

Applies the configuration parameters and IP address of an SNMPv3 management station (from the `params` *`params_name`* value configured with the `snmpv3 targetaddress` command in Step 5) to a specified SNMPv3 user (from the `user` *`user_name`* value configured with the `snmpv3 user` command in Step 2).

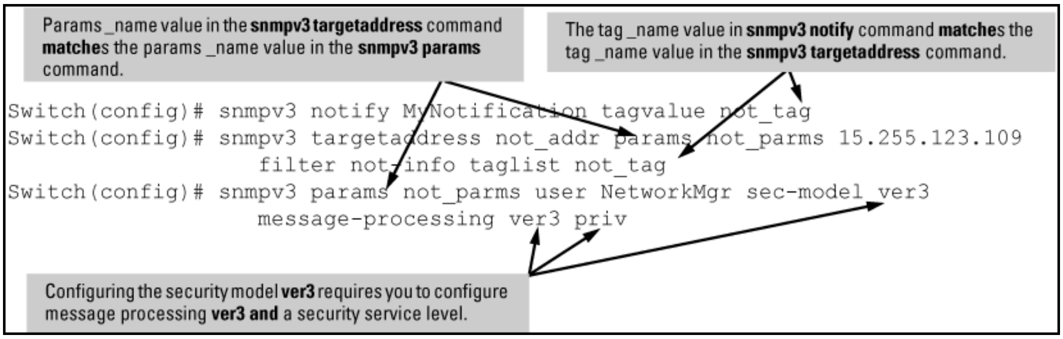
If you enter the `snmpv3 params user` command, you must also configure a security model (`sec-model`) and message processing algorithm (`msg-processing`).

`[ sec-model [ ver1 | ver2c | ver3 ] ]`	Configures the security model used for SNMPv3 notification messages sent to the management station configured with the `snmpv3 targetaddress` command in Step 5. If you configure the security model as `ver3`, you must also configure the message processing value as `ver3`.
`[ msg-processing ver1 | ver2c | ver3 [ noaut | auth | priv ] ]`	Configures the algorithm used to process messages sent to the SNMPv3 target address. If you configure the message processing value as `ver3` and the security model as `ver3`, you must also configure a security services level (`noauth`, `auth`, or `priv`).

Example

An example of how to configure SNMPv3 notification is shown here:

Figure 83 Example of an SNMPv3 notification configuration



Params_name value in the **snmpv3 targetaddress** command **matches** the params _name value in the **snmpv3 params** command.

The tag _name value in **snmpv3 notify** command **matches** the tag _name value in the **snmpv3 targetaddress** command.

```
Switch(config)# snmpv3 notify MyNotification tagvalue not_tag
Switch(config)# snmpv3 targetaddress not_addr params not_parms 15.255.123.109
                   filter not_info taglist not_tag
Switch(config)# snmpv3 params not_parms user NetworkMgr sec-model ver3
                   message-processing ver3 priv
```

Configuring the security model **ver3** requires you to configure message processing **ver3 and** a security service level.

Enabling or disabling notification/traps for network security failures and other security events (CLI)

For more information, see "Network security notifications" (page 223).

Syntax:

`[no]snmp-server enable traps [ snmp-auth | password-change-mgr | login-failure-mgr | port-security | auth-server-fail | dhcp-snooping | arp-protect | running-config-change ]`

Enables or disables sending one of the security notification types listed below to configured trap receivers. (Unless otherwise stated, all of the following notifications are enabled in the default configuration.)

The notification sends a trap:

`arp-protect`	If ARP packets are received with an invalid source or destination MAC address, an invalid IP address, or an invalid IP-to-MAC binding.
`auth-server-fail`	If the connection with a RADIUS or TACACS+ authentication server fails.

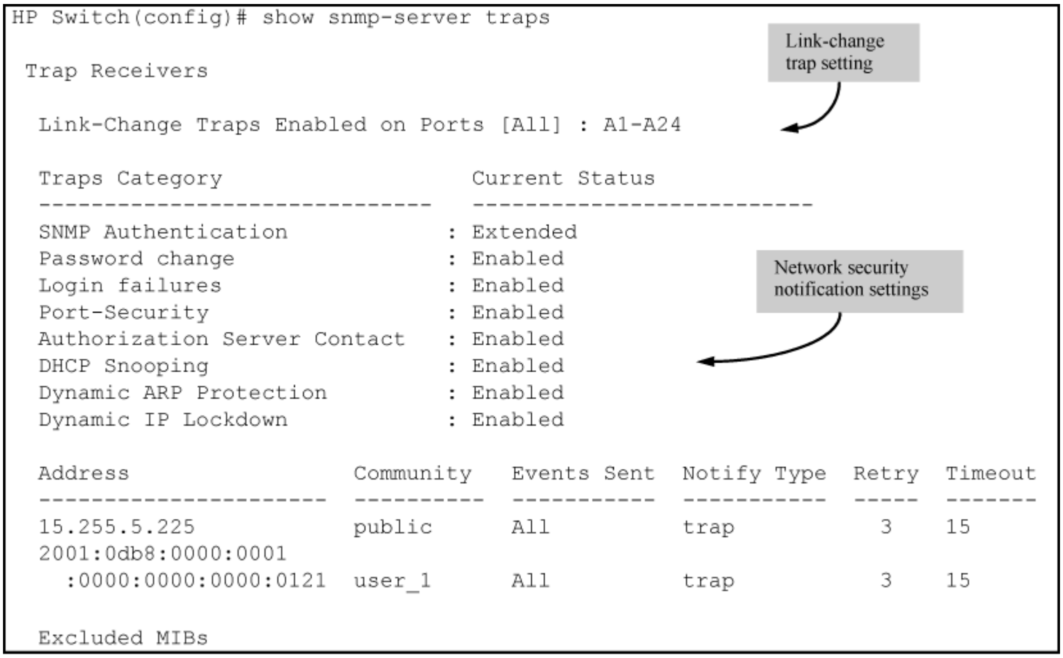
dhcp-snooping	If DHCP packets are received from an untrusted source or if DHCP packets contain an invalid IP-to-MAC binding.
dyn-ip-lockdown	If the switch is out of hardware resources needed to program a dynamic IP lockdown rule
link-change *port-list*	When the link state on a port changes from up to down, or the reverse.
login-failure-mgr	For a failed login with a manager password.
password-change-mgr	When a manager password is reset.
mac-notify	Globally enables the generation of SNMP trap notifications upon MAC address table changes.
port-security	For a failed authentication attempt through a web, MAC, or 801.X authentication session.
running-config-change	When changes to the running configuration file are made.
snmp-authentication [extended | standard]	For a failed authentication attempt via SNMP. (Default: extended.)
Startup-config-change	Sends a trap when changes to the startup configuration file are made. See “Enabling SNMP Traps on Startup Configuration Changes” on page 6–34. (Default: Disabled)

To determine the specific cause of a security event, check the Event Log in the console interface to see why a trap was sent. For more information, see "Using the Event Log for Troubleshooting Switch Problems" on page C-28.

Viewing the current configuration for network security notifications (CLI)

Enter the `show snmp-server traps` command, as shown in Figure 84 (page 183). Note that command output is a subset of the information displayed with the `show snmp-server` command in Figure 93 (page 189).

Figure 84 Display of configured network security notifications



```
HP Switch(config)# show snmp-server traps

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : A1-A24

  Traps Category                   Current Status
  ------------------------------   --------------------------
  SNMP Authentication            : Extended
  Password change                : Enabled
  Login failures                 : Enabled
  Port-Security                  : Enabled
  Authorization Server Contact   : Enabled
  DHCP Snooping                  : Enabled
  Dynamic ARP Protection         : Enabled
  Dynamic IP Lockdown            : Enabled

  Address                  Community   Events Sent  Notify Type  Retry  Timeout
  -----------------------  ----------  -----------  -----------  -----  -------
  15.255.5.225             public      All          trap             3  15
  2001:0db8:0000:0001
    :0000:0000:0000:0121   user_1      All          trap             3  15

  Excluded MIBs
```

Enabling Link-Change Traps (CLI)

By default, a switch is enabled to send a trap when the link state on a port changes from up to down (linkDown) or down to up (linkUp). To reconfigure the switch to send link-change traps to configured trap receivers, enter the `snmp-server enable traps link-change` command.

Syntax:

[no] `snmp-server enable traps link-change`*`port-list`*`[ all ]`

Enables or disables the switch to send a link-change trap to configured trap receivers when the link state on a port goes from up to down or down to up.

Enter `all` to enable or disable link-change traps on all ports on the switch.

Enabling SNMP traps on running configuration changes (CLI)

For more information, see "Enabling SNMP traps on running configuration changes" on page 14-93

Syntax:

[no] `snmp-server enable traps running-config-change[ transmission-interval 0-4294967295 ]`

Enables SNMP traps being sent when changes to the running configuration file are made.

(Default: Disabled)

`transmission-interval 0-2147483647` controls the egress rate for generating SNMP traps for the running configuration file. The value configured specifies the time interval in seconds that is allowed between the transmission of two consecutive traps.

None of the running configuration change events that occur within the specified interval generate SNMP traps, although they are logged in the Configuration Changes History Table.

A value of 0 (zero) means there is no limit; traps can be sent for every running configuration change event.

(Default: Zero)

Enabling SNMP traps on Startup Configuration changes

You can send a specific SNMP trap for any configuration change made in the switch's startup configuration file when the change is written to flash. Changes to the configuration file can occur when executing a CLI write command, executing an SNMP set command directly using SNMP, or when using the WebAgent

NOTE: A log message is always generated when a startup configuration change occurs. An example log entry is:

```
I 07/06/10 18:21:39 02617 mgr: Startup configuration changed by SNMP.
New seq. number 8
```

The corresponding trap message is sent if the snmp-server enable traps startupconfig- change command is configured.

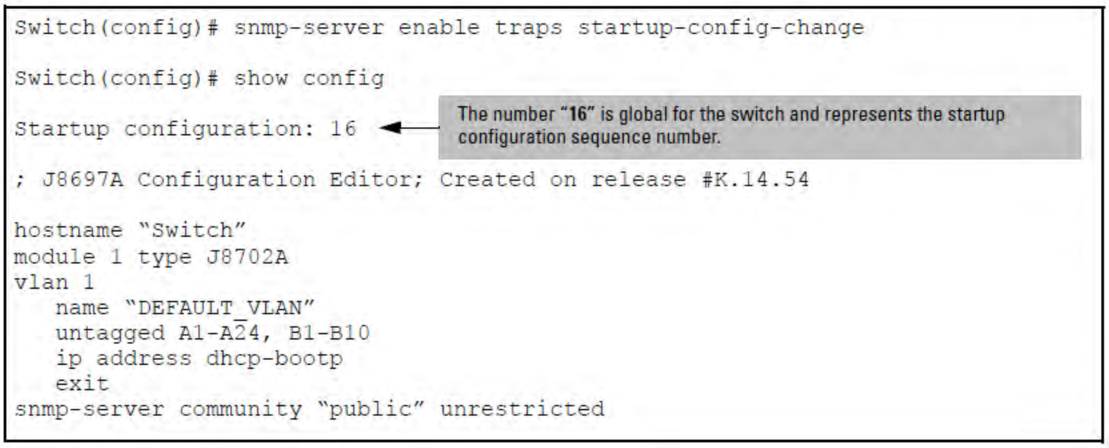
Syntax

[no]`snmp-server enable traps startup-config-change`

Enables notification of a change to the startup configuration. The change event is logged. Default: Disabled

An example of configuring the command from the CLI is shown in Figure 6-16. The number that displays when show config is executed is global for the switch and represents the startup configuration sequence number.

Figure 85 Enabling notification of changes to the Startup Configuration file

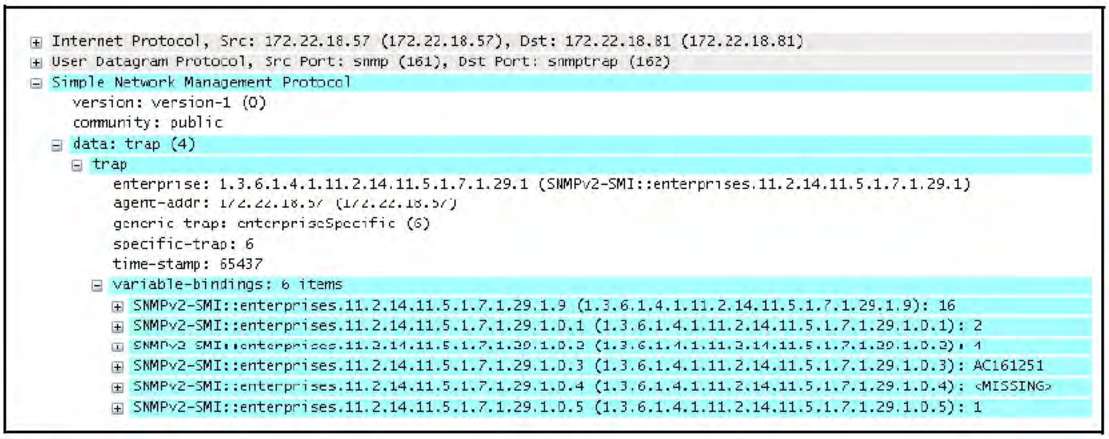


```
Switch(config)# snmp-server enable traps startup-config-change

Switch(config)# show config

Startup configuration: 16

; J8697A Configuration Editor; Created on release #K.14.54

hostname "Switch"
module 1 type J8702A
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A24, B1-B10
   ip address dhcp-bootp
   exit
snmp-server community "public" unrestricted
```

The number "16" is global for the switch and represents the startup configuration sequence number.

Figure 6-17 displays an example o f the fields in the trap when a change is made via SNMP (station ip=0xAC161251 (172.22.18.81), no username is set, and the new sequence number is 16).

Figure 86 Fields when the SNMP trap is set



```
⊞ Internet Protocol, Src: 172.22.18.57 (172.22.18.57), Dst: 172.22.18.81 (172.22.18.81)
⊞ User Datagram Protocol, Src Port: snmp (161), Dst Port: snmptrap (162)
⊟ Simple Network Management Protocol
    version: version-1 (0)
    community: public
  ⊟ data: trap (4)
    ⊟ trap
        enterprise: 1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1 (SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1)
        agent-addr: 172.22.18.57 (172.22.18.57)
        generic trap: enterpriseSpecific (6)
        specific-trap: 6
        time-stamp: 65437
      ⊟ variable-bindings: 6 items
        ⊞ SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.9 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.9): 16
        ⊞ SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.1 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.1): 2
        ⊞ SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.2 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.2): 4
        ⊞ SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.3 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.3): AC161251
        ⊞ SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.4 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.4): <MISSING>
        ⊞ SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.5 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.5): 1
```

Viewing configuration file change information (CLI)

Syntax:

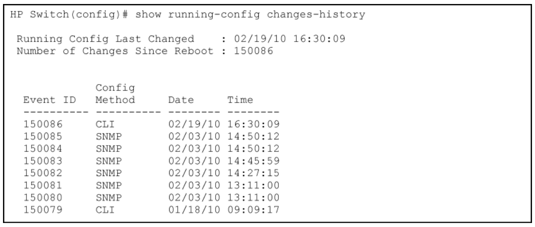
`show running-config[ changes-history [ 1-32 ] ][ detail ]`

Displays the history up to 32 events for changes made to the running-configuration file, as shown in Figure 87 (page 186) and Figure 88 (page 186). The changes are displayed in descending order, the most recent change at the top of the list. You can specify from 1 to 32 entries for display.

The `detail` option displays a more detailed amount of information for the configuration changes. Figure 89 (page 186) and Figure 90 (page 186) display detailed information for configuration changes history.

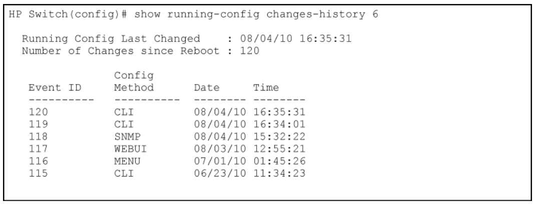
Examples

Figure 87 Example of output for running configuration changes history for all ports



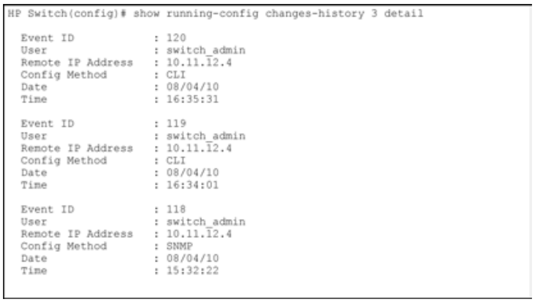
```
HP Switch(config)# show running-config changes-history

 Running Config Last Changed    : 02/19/10 16:30:09
 Number of Changes Since Reboot : 150086


             Config
  Event ID   Method     Date     Time
  ---------- ---------- -------- --------
  150086     CLI        02/19/10 16:30:09
  150085     SNMP       02/03/10 14:50:12
  150084     SNMP       02/03/10 14:50:12
  150083     SNMP       02/03/10 14:45:59
  150082     SNMP       02/03/10 14:27:15
  150081     SNMP       02/03/10 13:11:00
  150080     SNMP       02/03/10 13:11:00
  150079     CLI        01/18/10 09:09:17
```

Figure 88 Example of output for running configuration changes history



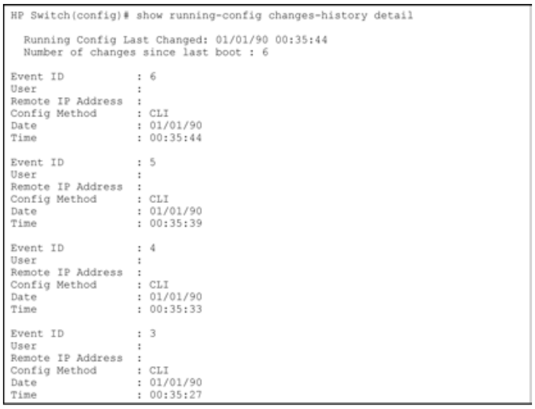
```
HP Switch(config)# show running-config changes-history 6

  Running Config Last Changed    : 08/04/10 16:35:31
  Number of Changes since Reboot : 120

             Config
   Event ID     Method      Date     Time
   ----------   ----------  -------- --------
   120          CLI         08/04/10 16:35:31
   119          CLI         08/04/10 16:34:01
   118          SNMP        08/04/10 15:32:22
   117          WEBUI       08/03/10 12:55:21
   116          MENU        07/01/10 01:45:26
   115          CLI         06/23/10 11:34:23
```

Figure 89 Example of detailed output for running configuration changes history



```
HP Switch(config)# show running-config changes-history 3 detail

  Event ID              : 120
  User                  : switch_admin
  Remote IP Address     : 10.11.12.4
  Config Method         : CLI
  Date                  : 08/04/10
  Time                  : 16:35:31

  Event ID              : 119
  User                  : switch_admin
  Remote IP Address     : 10.11.12.4
  Config Method         : CLI
  Date                  : 08/04/10
  Time                  : 16:34:01

  Event ID              : 118
  User                  : switch_admin
  Remote IP Address     : 10.11.12.4
  Config Method         : SNMP
  Date                  : 08/04/10
  Time                  : 15:32:22
```

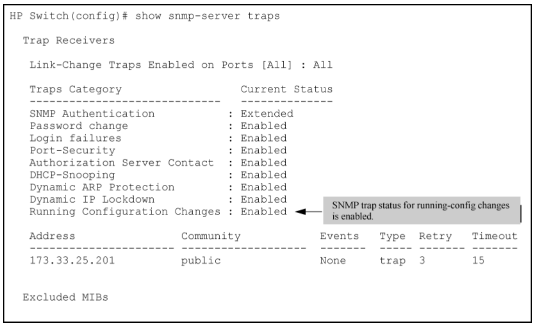
Figure 90 Example of output for running config changes history with detail



```
HP Switch(config)# show running-config changes-history detail

  Running Config Last Changed: 01/01/90 00:35:44
  Number of changes since last boot : 6

Event ID             : 6
User                 :
Remote IP Address    :
Config Method        : CLI
Date                 : 01/01/90
Time                 : 00:35:44

Event ID             : 5
User                 :
Remote IP Address    :
Config Method        : CLI
Date                 : 01/01/90
Time                 : 00:35:39

Event ID             : 4
User                 :
Remote IP Address    :
Config Method        : CLI
Date                 : 01/01/90
Time                 : 00:35:33

Event ID             : 3
User                 :
Remote IP Address    :
Config Method        : CLI
Date                 : 01/01/90
Time                 : 00:35:27
```

Figure 91 (page 187) displays the current status (enabled/disabled) of the SNMP trap type for running-configuration changes.

Figure 91 Example of SNMP trap configuration status information



```
HP Switch(config)# show snmp-server traps

  Trap Receivers

   Link-Change Traps Enabled on Ports [All] : All

   Traps Category                  Current Status
   -----------------------------   --------------
   SNMP Authentication           : Extended
   Password change               : Enabled
   Login failures                : Enabled
   Port-Security                 : Enabled
   Authorization Server Contact  : Enabled
   DHCP-Snooping                 : Enabled
   Dynamic ARP Protection        : Enabled
   Dynamic IP Lockdown           : Enabled
   Running Configuration Changes : Enabled

   Address                Community            Events   Type  Retry   Timeout
   ---------------------- -------------------  -------  ----- ------- -------
   173.33.25.201          public               None     trap  3       15


  Excluded MIBs
```

SNMP trap status for running-config changes is enabled.

Configuring the source IP address for SNMP notifications (CLI)

For more information, see “Source IP address for SNMP notifications” (page 224).

Syntax:

[no] `snmp-server response-source` [`dst-ip-of-request` [*`ipv4-addr`* | *`ipv6-addr`*] | `loopback0-7`]

Specifies the source IP address of the SNMP response PDU. The default SNMP response PDU uses the IP address of the active interface from which the SNMP response was sent as the source IP address.

The `no` form of the command resets the switch to the default behavior (compliant with rfc-1517).

(Default: Interface IP address)

`dst-ip-of-request`	Destination IP address of the SNMP request PDU that is used as the source IP address in an SNMP response PDU.
`[ ipv4-addr | ipv6-addr ]`	User-defined interface IP address that is used as the source IP address in an SNMP response PDU. Both IPv4 and IPv6 addresses are supported.
`loopback 0-7`	IP address configured for the specified loopback interface that is used as the source IP address in an SNMP response PDU. If multiple loopback IP addresses are configured, the lowest alphanumeric address is used.

Example

To use the IP address of the destination interface on which an SNMP request was received as the source IP address in the IP header of SNMP traps and replies, enter the following command:

```
HP Switch(config)# snmp-server response-source dst-ip-of-request
```

Syntax:

[no] `snmp-server trap-source` [*`ipv4-addr`* | `loopback0-7`]

Specifies the source IP address to be used for a trap PDU. To configure the switch to use a specified source IP address in generated trap PDUs, enter the `snmp-server trap-source` command.

The `no` form of the command resets the switch to the default behavior (compliant with rfc-1517).

(Default: Use the interface IP address in generated trap PDUs)

ipv4-addr	User-defined interface IPv4 address that is used as the source IP address in generated traps. IPv6 addresses are not supported.
`loopback 0-7`	P address configured for the specified loopback interface that is used as the source IP address in a generated trap PDU. If multiple loopback IP addresses are configured, the lowest alphanumeric address is used.

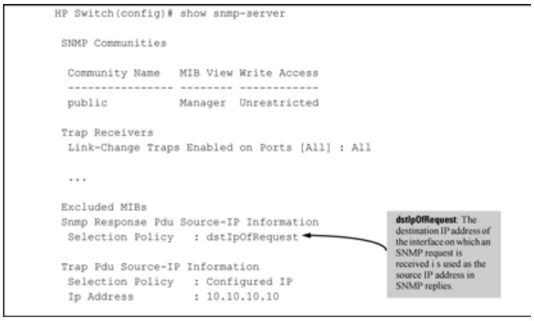
NOTE: When you use the `snmp-server response-source` and `snmp-server trap-source` commands, note the following behavior:

- The `snmp-server response-source` and `snmp-server trap-source` commands configure the source IP address for IPv4 interfaces only.
- You must manually configure the `snmp-server response-source` value if you wish to change the default user-defined interface IP address that is used as the source IP address in SNMP traps (RFC 1517).
- The values configured with the `snmp-server response-source` and `snmp-server trap-source` commands are applied globally to all interfaces that are sending SNMP responses or SNMP trap PDUs.
- Only the source IP address field in the IP header of the SNMP response PDU can be changed.
- Only the source IP address field in the IP header and the SNMPv1 Agent Address field of the SNMP trap PDU can be changed.

Verifying the configuration of the interface IP address used as the source IP address in IP headers for SNMP replies and traps sent from the switch (CLI)

Enter the `show snmp-server` command to display the SNMP policy configuration, as shown in Figure 92 (page 188).

Figure 92 Display of source IP address configuration



```
HP Switch(config)# show snmp-server

 SNMP Communities

  Community Name   MIB View Write Access
  ---------------- -------- ------------
  public           Manager  Unrestricted

 Trap Receivers
  Link-Change Traps Enabled on Ports [All] : All

  ...

 Excluded MIBs
 Snmp Response Pdu Source-IP Information
  Selection Policy   : dstIpOfRequest

 Trap Pdu Source-IP Information
  Selection Policy   : Configured IP
  Ip Address         : 10.10.10.10
```

dstIpOfRequest: The destination IP address of the interface on which an SNMP request is received i s used as the source IP address in SNMP replies.

Viewing SNMP notification configuration (CLI)

Syntax:

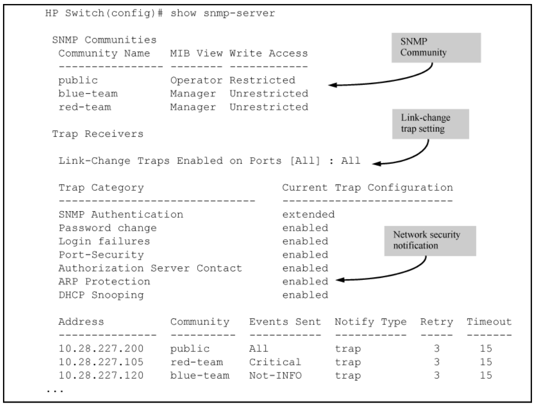
`show snmp-server`

Displays the currently configured notification settings for versions SNMPv1 and SNMPv2c traps, including SNMP communities, trap receivers, link-change traps, and network security notifications.

Example

In the following example, the `show snmp-server` command output shows that the switch has been configured to send SNMP traps and notifications to management stations that belong to the "public," "red-team," and "blue-team" communities.

Figure 93 Display of SNMP notification configuration



```
HP Switch(config)# show snmp-server

 SNMP Communities
  Community Name   MIB View Write Access
  ---------------- -------- ------------
  public           Operator Restricted
  blue-team        Manager  Unrestricted
  red-team         Manager  Unrestricted

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : All

  Trap Category                     Current Trap Configuration
  ------------------------------    --------------------------
  SNMP Authentication               extended
  Password change                   enabled
  Login failures                    enabled
  Port-Security                     enabled
  Authorization Server Contact      enabled
  ARP Protection                    enabled
  DHCP Snooping                     enabled

  Address          Community  Events Sent  Notify Type  Retry  Timeout
  ---------------- ---------- -----------  -----------  -----  -------
  10.28.227.200    public     All          trap           3      15
  10.28.227.105    red-team   Critical     trap           3      15
  10.28.227.120    blue-team  Not-INFO     trap           3      15
...
```

Configuring the MAC address count option

The MAC Address Count feature provides a way to notify the switch management system when the number of MAC addresses learned on a switch port exceeds the permitted configurable number.

To enable the mac-count-notify option, enter this command in global config context.

Syntax

`[no]snmp-server enable traps mac-count-notify`

Sends a trap when the number of MAC addresses learned on the specified ports exceeds the configured `<learned-count>` value.

To configure the mac-count-notify option on a port or ports, enter this command. When the configured number of MAC addresses is exceeded (the learned-count), a trap is sent.

Syntax

`[no]mac-count-notify traps <port-list> [<learned-count>]`

Configures `mac-count-notify traps` on the specified ports (or all) for the entire switch.

The `[no]` form of the command disables `mac-count-notify traps`.

`[<learned-count>]`: The number of MAC addresses learned before sending a trap. Values range between 1-128.

Default: 32

Example configuring mac-count notify traps on ports 5–7

```
HP Switch (config)# mac-count-notify traps 5-7 50
```

Displaying information about the mac-count-notify option

Use the show mac-count-notify traps [<port-list>] command to display information about the configured value for sending a trap, the current count, and if a trap has been sent.

Example of information displayed for `show mac-count-notify traps` command

```
HP Siwtch (config)# show mac-count-notify traps

Mac-count-notify Enabled: Yes

Port                Count for          Count            Trap Sent
                    sending Trap
-----------------------------------------------------------------
1
2
3
4
5                    50                    0              No
6                    50                    2              No
7                    50                    0              No
8
9
...
```

The interface context can be used to configure the value for sending a trap.

Example of configuring mac-count-notify traps from the interface context

```
HP Switch (config)# interface 5
```

```
HP Switch (eth-5)# mac-count-notify traps 35
```

The `show snmp-server traps` command displays whether the MAC Address Count feature is enabled or disabled.

Example of information about SNMP traps, including MAC address count being Enabled/Disabled

```
HP Switch(config)# show snmp-server traps
Trap Receivers
Link-Change Traps Enabled on Ports [All] : All
Traps Category                Current Status
_____________________________ __________________
SNMP Authentication :             Extended
Password change :                 Enabled
Login failures :                  Enabled
Port-Security :                   Enabled
Authorization Server Contact :    Enabled
DHCP-Snooping :                   Enabled
Dynamic ARP Protection :          Enabled
Dynamic IP Lockdown :             Enabled
MAC address table changes :       Disabled
MAC Address Count :               Enabled

Address                  Community             Events   Type   Retry  Timeout
---------------------- ---------------------- -------- ------ ------- -------
15.146.194.77            public                 None    trap     3      15
15.255.134.252           public                 None    trap     3      15
16.181.49.167            public                 None    trap     3      15
16.181.51.14             public                 None    trap     3      15
Excluded MIBs
```

Configuring the MAC address table change option

When enabled, this feature allows the generation of SNMP traps for each MAC address table change. Notifications can be generated for each device that connects to a port and for devices that are connected through another device (daisy-chained).

The `snmp-server enable traps mac-notify` command globally enables the generation of SNMP trap notifications upon MAC address table changes.

Syntax

```
[no]snmp-server enable traps mac-notify [mac-move |
trap-interval <0- 120>]
```

Globally enables or disables generation of SNMP trap notifications.

trap-interval	The time interval (in seconds) that trap notifications are sent. A value of zero disables the interval and traps are sent as events occur. If the switch is busy, notifications can be sent prior to the configured interval. Notifications may be dropped in extreme instances and a system warning is logged.The range is 0-120 seconds. Default: 30 seconds.
mac-move	Configures the switch to capture data for MAC addresses that are moved from one port to another port. The `snmp-server enable traps mac-notify` command must have been enabled in order for this information to be sent as an SNMP notification.

Example of trap-interval option

```
HP Switch (config)# snmp-server enable traps mac-notify
trap-interval 60
```

Example of mac-move option

```
HP Switch (config)# snmp-server enable traps mac-notify mac-move
```

Additional mac-notify options for per-port Mac changes

Use the following command to configure SNMP traps for learned or removed MAC addresses on a per-port basis.

NOTE: The switch will capture learned or removed events on the selected ports, but will not send an SNMP trap unless mac-notify has been enabled with the `snmp-server enable traps mac-notify` command.

Syntax

```
[no]mac-notify traps <port-list>[learned | removed]
```

When this command is executed without the **learned** or **removed** option, it enables or disables the capture of both learned and removed MAC address table changes for the selected ports in <port-list>

<port-list>	Configures MAC address table changes capture on the specified ports. Use all to capture changes for all ports on the switch.
learned	Enables the capture of learned MAC address table changes on the selected ports.
removed	Enables the capture of removed MAC address table changes table on the selected ports.

Example of configuring traps on a per-port basis for learned MAC addresses

```
HP Switch(config)# mac-notify traps 5-6 learned
HP Switch(config)# show mac-notify traps 5-6
Mac Notify Trap Information
Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60
Port    MAC Addresses    trap learned/removed
------ ----------------------------------
5       Learned
6       Learned
```

Example of configuring traps on a port-bases for removed MAC addresses

```
HP Switch(config)# mac-notify traps 3-4 removed
Switch(config)# show mac-notify traps
Mac Notify Trap Information
Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60
Port    MAC Addresses    trap learned/removed
------ ----------------------------------
1         None
2         None
3         Removed
4         Removed
```

Configuring the mac-notify option at the interface context level

You can also execute the `mac-notify traps` command from the interface context.

Example of the interface context for MAC-notify traps command

```
HP Switch(config)# int 11
HP Switch(int-11)# mac-notify traps learned
```

Viewing `mac-notify traps` configuration information

Use the `show mac-notify traps` command to display information about SNMP trap configuration for MAC Address Table changes.

Syntax

```
show mac-notify traps [port-list]
```

Example of information for SNMP trap configuration

Displays SNMP trap information for all ports, or each port in the port-list.

```
HP Switch(config)# show mac-notify traps
Mac Notify Trap Information
Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60
Port     MAC Addresses    trap learned/removed
------ ----------------------------------
1        None
2        None
3        Removed
4        Removed
5        Learned
6        Learned
```

The configured `mac-notify` commands are displayed in the `show running-configuration` output.

Example of running config file with mac-notify parameters configured

```
HP Switch(config)# show running-config
Running configuration:
; J9087A Configuration Editor; Created on release #R.11.XX
hostname "Switch"
snmp-server community "public" Unrestricted
snmp-server host 15.255.133.236 "public"
snmp-server host 15.255.133.222 "public"
snmp-server host 15.255.133.70 "public"
snmp-server host 15.255.134.235 "public"
```

```
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-28
  ip address dhcp-bootp
  exit
snmp-server enable traps mac-notify mac-move
snmp-server enable traps mac-notify trap-interval 60
snmp-server enable traps mac-notify
mac-notify traps 5-6 learned
mac-notify traps 3-4 removed
```

Configuring listening mode (CLI)

For more information, "See About configuring listening mode”

Syntax:

`snmp-server [ listen [ oobm | data | both ] ]`

Enables or disables inbound SNMP access on a switch.

Use the `no` version of the command to disable inbound SNMP access.

The `listen` parameter is available only on switches that have a separate out-of-band management port. Values for this parameter are:

`oobm`	Inbound SNMP access is enabled only on the out-of-band management port.
`data`	Inbound SNMP access is enabled only on the data ports.
`both`	Inbound SNMP access is enabled on both the out-of-band management port and on the data ports. This is the default value.

For more information on out-of-band management, see Appendix I, "Network Out-of-Band Management" in this guide.

The `listen` parameter is not available on switches that do not have a separate out-of-band management port.

Configuring sFlow (CLI)

The following sFlow commands allow you to configure sFlow instances via the CLI. For more information, see “Advanced management: RMON” (page 225).

Syntax:

[no] `sflow` *`receiver-instance`* `destination` *`ip-address`* [*`udp-port-num`*]

Enables an sFlow receiver/destination. The receiver-instance number must be a 1, 2, or 3.

By default, the udp destination port number is 6343.

To disable an sFlow receiver/destination, enter `no sflow` *`receiver-instance`*.

Syntax:

`sflow` *`receiver-instance`* `sampling` *`port-list sampling rate`*

Once an sFlow receiver/destination has been enabled, this command enables flow sampling for that instance. The receiver-instance number is 1, 2, or 3, and the sampling rate is the allowable non-zero skipcount for the specified port or ports.

To disable flow-sampling for the specified port-list, repeat the above command with a sampling rate of `0`.

Syntax:

`sflow` *`receiver-instance`* `polling` *`port-list polling interval`*

Once an sFlow receiver/destination has been enabled, this command enables counter polling for that instance. The receiver-instance number is 1, 2, or 3, and the polling interval may be set to an allowable non-zero value to enable polling on the specified port or ports.

To disable counter-polling for the specified port-list, repeat the above command with a polling interval of `0`.

NOTE: Under the multiple instance implementation, sFlow can be configured via the CLI or via SNMP. However, CLI-owned sFlow configurations cannot be modified via SNMP, whereas SNMP-owned instances can be disabled via the CLI using the `no sflow` *`receiver-instance`* command.

Viewing sFlow Configuration and Status (CLI)

The following sFlow commands allow you to display sFlow configuration and status via the CLI. Figure 95 (page 194) is an example of `sflow agent` information.

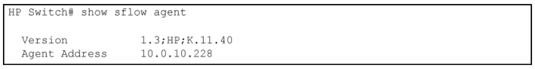
Syntax:

`show sflow agent`

Displays sFlow agent information. The agent address is normally the IP address of the first VLAN configured.

The `show sflow agent` command displays read-only switch agent information. The version information shows the sFlow version, MIB support, and software versions; the agent address is typically the IP address of the first VLAN configured on the switch.

Figure 94 Example of viewing `sflow agent` information



```
HP Switch# show sflow agent

  Version          1.3;HP;K.11.40
  Agent Address    10.0.10.228
```

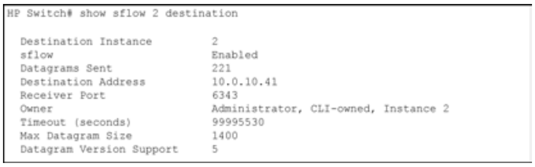
Syntax:

`show sflow` *`receiver instance`* `destination`

Displays information about the management station to which the sFlow sampling-polling data is sent.

The `show sflow` *`instance`* `destination` command includes information about the management-station's destination address, receiver port, and owner, as shown in Figure 95 (page 194).

Figure 95 Example of viewing `sFlow destination` information



```
HP Switch# show sflow 2 destination

  Destination Instance        2
  sflow                       Enabled
  Datagrams Sent              221
  Destination Address         10.0.10.41
  Receiver Port               6343
  Owner                       Administrator, CLI-owned, Instance 2
  Timeout (seconds)           99995530
  Max Datagram Size           1400
  Datagram Version Support    5
```

Note the following details:

- **Destination Address** remains blank unless it has been configured.
- **Datagrams Sent** shows the number of datagrams sent by the switch agent to the management station since the switch agent was last enabled.

- **Timeout** displays the number of seconds remaining before the switch agent will automatically disable sFlow (this is set by the management station and decrements with time).
- **Max Datagram Size** shows the currently set value (typically a default value, but this can also be set by the management station).

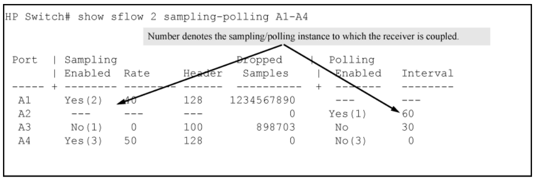
Syntax:

`show sflow` *`receiver instance`* `sampling-polling` *`port-list/range`*

Displays status information about sFlow sampling and polling.

The `show sflow` *`instance`* `sampling-polling [`*`port-list`*`]` command displays information about sFlow sampling and polling on the switch, as shown in Figure 96 (page 195). You can specify a list or range of ports for which to view sampling information.

Figure 96 Example of viewing sFlow sampling and polling information



```
HP Switch# show sflow 2 sampling-polling A1-A4

 Port   | Sampling                          Dropped     |  Polling
        | Enabled  Rate       Header   Samples      |   Enabled    Interval
 ----- + -------- -------- ------  ----------  +  -------    --------
  A1      Yes(2)   40         128    1234567890      ---        ---
  A2       ---     ---        ---             0     Yes(1)      60
  A3       No(1)    0         100        898703      No         30
  A4      Yes(3)   50         128             0      No(3)       0
```

Number denotes the sampling/polling instance to which the receiver is coupled.

NOTE: The sampling and polling instances (noted in parentheses) coupled to a specific receiver instance are assigned dynamically, and so the instance numbers may not always match. The key thing to note is whether sampling or polling is enabled on a port, and the sampling rates or polling intervals for the receiver instance configured on each port.

Displaying the global LLDP, port admin, and SNMP notification status (CLI)

In the default configuration, LLDP is enabled and in both transmit and receive mode on all active ports. The LLDP configuration includes global settings that apply to all active ports on the switch, and per-port settings that affect only the operation of the specified ports.

The commands in this section affect both LLDP and LLDP-MED operation. for information on operation and configuration unique to LLDP-MED, refer to “LLDP-MED (Media-Endpoint-Discovery)” on page 6-74.

Syntax:

`show lldp config`

Displays the LLDP global configuration, LLDP port status, and SNMP notification status. For information on port admin status, see“Configuring per-port transmit and receive modes (CLI)” (page 199).

Example of viewing the general LLDP configuration

`show lldp config` produces the following display when the switch is in the default LLDP configuration:

```
HP Switch(config)# show lldp config

LLDP Global Configuration

LLDP Enabled [Yes] :            Yes
LLDP Transmit Interval [30] :   30
LLDP Hold time Multiplier [4] : 4
LLDP Delay Interval [2] :       2
LLDP Reinit Interval [2] :      2
LLDP Notification Interval [5] : 5
LLDP Fast Start Count [5] :     5
LLDP Port Configuration
Port | AdminStatus NotificationEnabled  Med Topology Trap Enabled
---- + ----------- -------------------  -------------------------
A1 |    Tx_Rx        False              False
A2 |    Tx_Rx        False              False
A3 |    Tx_Rx        False              False
A4 |    Tx_Rx        False              False
A5 |    Tx_Rx        False              False
A6 |    Tx_Rx        False              False
A7 |    Tx_Rx        False              False
A8 |    Tx_Rx        False              False
```

NOTE: The values displayed in the LLDP column correspond to the `lldp refresh-interval` command

Viewing port configuration details (CLI)

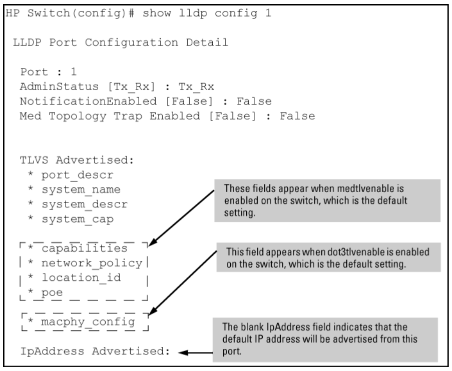
Syntax:

`show lldp config` *`port-list`*

Displays the LLDP port-specific configuration for all ports in *`port-list`*, including which optional TLVs and any non-default IP address that are included in the port's outbound advertisements.

For information on the notification setting, see "SNMP notification support" (page 230). For information on the other configurable settings displayed by this command, see "Configuring per-port transmit and receive modes (CLI)" (page 199).

Figure 97 Per-port configuration display



```
HP Switch(config)# show lldp config 1

 LLDP Port Configuration Detail

  Port : 1
  AdminStatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False


  TLVS Advertised:
   * port_descr
   * system_name
   * system_descr
   * system_cap

   * capabilities
   * network_policy
   * location_id
   * poe

   * macphy_config

  IpAddress Advertised:
```

These fields appear when medtlvenable is enabled on the switch, which is the default setting.

This field appears when dot3tlvenable is enabled on the switch, which is the default setting.

The blank IpAddress field indicates that the default IP address will be advertised from this port.

Enabling or disabling LLDP operation on the switch (CLI)

For more information, see "LLDP operation on the switch" (page 230).

Syntax:

`[no] lldp run`

Enables or disables LLDP operation on the switch.

The `no` form of the command, regardless of individual LLDP port configurations, prevents the switch from transmitting outbound LLDP advertisements and causes the switch to drop all LLDP advertisements received from other devices.

The switch preserves the current LLDP configuration when LLDP is disabled. After LLDP is disabled, the information in the LLDP neighbors database remains until it times-out.

(Default: Enabled)

Example

To disable LLDP on the switch:

```
HP Switch(config)# no lldp run
```

Changing the packet transmission interval (CLI)

This interval controls how often active ports retransmit advertisements to their neighbors.

Syntax:

`lldp refresh-interval  5 - 32768`

Changes the interval between consecutive transmissions of LLDP advertisements on any given port.

(Default: 30 seconds)

NOTE: The `refresh-interval` must be greater than or equal to (4 x `delay-interval`). (The default `delay-interval` is 2). For example, with the default `delay-interval`, the lowest `refresh-interval`you can use is 8 seconds (4 x 2=8). Thus, if you want a `refresh-interval` of 5 seconds, you must first change the delay interval to 1 (that is, 4 x 1 5). If you want to change the `delay-interval`, use the `setmib` command.

Changing the time-to-live for transmitted advertisements (CLI)

For more information, see "Time-to-Live for transmitted advertisements" (page 230).

Syntax:

`lldp holdtime-multiplier  2 - 10`

Changes the multiplier an LLDP switch uses to calculate the Time-to-Live for the LLDP advertisements it generates and transmits to LLDP neighbors. When the Time-to-Live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.

(Default: 4; Range 2–10)

Example

If the refresh-interval on the switch is 15 seconds and the `holdtime-multiplier` is at the default, the Time-to-Live for advertisements transmitted from the switch is 60 seconds (4 x 15).

To reduce the Time-to-Live, you could lower the `holdtime-interval` to 2, which would result in a Time-to-Live of 30 seconds.

```
HP Switch(config)# lldp holdtime-multiplier 2
```

Changing the delay interval between advertisements generated by value or status changes to the LLDP MIB (CLI)

For more information, see "Delay interval between advertisements generated by value or status changes to the LLDP MIB" (page 230).

Syntax:

`setmib lldpTxDelay.0 -i  1 - 8192`

Uses `setmib` to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements because of a change in LLDP MIB content.

(Default: 2; Range 1–8192)

NOTE: The LLDP refresh-interval (transmit interval) must be greater than or equal to (4 x delay-interval). The switch does not allow increasing the delay interval to a value that conflicts with this relationship. That is, the switch displays `Inconsistent value` if (4 x delay-interval) exceeds the current transmit interval, and the command fails. Depending on the current refresh-interval setting, it may be necessary to increase the refresh-interval before using this command to increase the delay-interval.

NOTE: For the 5400zl, 3800, and 8200zl switches, when the switch is in enhanced secure mode, the following prompt appears before the sensitive information for the setmib command is displayed:

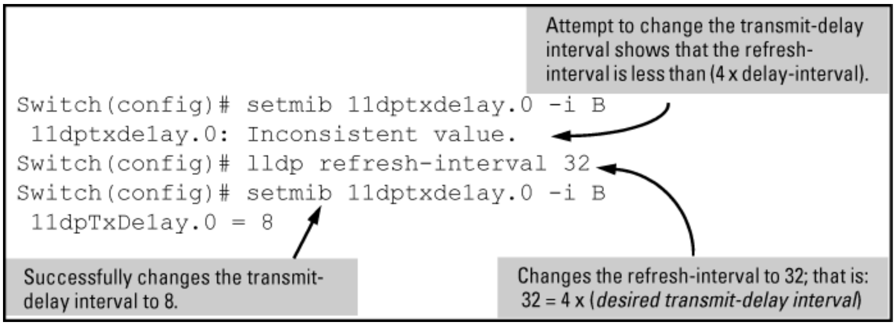
```
The setmib command should not be used in enhanced secure mode.
```

For more information, see the chapter "Secure Mode (5400zl. 3800, and 8200zl)" in the *Access Security Guide* for your switch.

Example

To change the delay-interval from 2 seconds to 8 seconds when the refresh-interval is at the default 30 seconds, you must first set the refresh-interval to a minimum of 32 seconds (32 = 4 x 8). (See Figure 98 (page 198).)

Figure 98 Changing the transmit-delay interval



```
Switch(config)# setmib 11dptxdelay.0 -i B
 11dptxdelay.0: Inconsistent value.
Switch(config)# lldp refresh-interval 32
Switch(config)# setmib 11dptxdelay.0 -i B
 11dpTxDelay.0 = 8
```

Attempt to change the transmit-delay interval shows that the refresh-interval is less than (4 x delay-interval).

Changes the refresh-interval to 32; that is: 32 = 4 x (*desired transmit-delay interval*)

Successfully changes the transmit-delay interval to 8.

Changing the reinitialization delay interval (CLI)

For more information, see "Reinitialization delay interval" (page 230).

Syntax:

```
setmib lldpReinitDelay.0 -i  1 - 10
```

Uses `setmib` to change the minimum time (reinitialization delay interval) an LLDP port will wait before reinitializing after receiving an LLDP disable command followed closely by a txonly or tx_rx command. The delay interval commences with execution of the `lldp admin-status port-list  disable` command.

(Default: 2 seconds; Range 1–10 seconds)

Example

The following command changes the reinitialization delay interval to five seconds:

```
HP Switch(config)# setmib lldpreinitdelay.0 -i 5
```

Enabling LLDP data change notification for SNMP trap receivers (CLI)

For more information, see Section 1.67.3.2.

Syntax:

```
[no] lldp enable-notification  port-list
```

Enables or disables each port in *port-list* for sending notification to configured SNMP trap receivers if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor.

(Default: Disabled)

For information on configuring trap receivers in the switch, see "SNMP notifications" (page 221).

Example

This command enables SNMP notification on ports 1 - 5:

```
HP Switch(config)# lldp enable-notification 1-5
```

Changing the minimum interval for successive data change notifications for the same neighbor

For more information, see "Changing the minimum interval for successive data change notifications for the same neighbor" (page 230).

Syntax:

```
setmib lldpnotificationinterval.0 -i  1 - 3600
```

Globally changes the interval between successive traps generated by the switch. If multiple traps are generated in the specified interval, only the first trap is sent. The remaining traps are suppressed. (A network management application can periodically check the switch MIB to detect any missed change notification traps. See IEEE P802.1AB or later for more information.)

(Default: 5 seconds)

Example

The following command limits change notification traps from a particular switch to one per minute.

```
HP Switch(config)# setmib lldpnotificationinterval.0 -i 60 lldpNotificationInterval.0=60
```

Configuring per-port transmit and receive modes (CLI)

Syntax:

```
lldp admin-status  port-list   txonly | rxonly | tx_rx | disable
```

With LLDP enabled on the switch in the default configuration, each port is configured to transmit and receive LLDP packets. These options enable you to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.

`txonly`	Configures the specified ports to transmit LLDP packets, but block inbound LLDP packets from neighbor devices.
`rxonly`	Configures the specified ports to receive LLDP packets from neighbors, but block outbound packets to neighbors.
`tx_rx`	Configures the specified ports to both transmit and receive LLDP packets. (This is the default setting.)
`disable`	Disables LLDP packet transmit and receive on the specified ports.

Configuring a remote management address for outbound LLDP advertisements (CLI)

This is an optional command you can use to include a specific IP address in the outbound LLDP advertisements for specific ports. For more information, see "Basic LLDP per-port advertisement content" (page 230).

Syntax:

```
[no] lldp config  port-list  ipAddrEnable  ip-address
```

Replaces the default IP address for the port with an IP address you specify. This can be any IP address configured in a static VLAN on the switch, even if the port does not belong to the VLAN configured with the selected IP address.

The no form of the command deletes the specified IP address.

If there are no IP addresses configured as management addresses, the IP address selection method returns to the default operation.

Default: The port advertises the IP address of the lowest-numbered VLAN (VID) to which it belongs. If there is no IP address configured on the VLANs to which the port belongs, and if the port is not configured to advertise an IP address from any other (static) VLAN on the switch, the port advertises an address of 127.0.0.1.)

NOTE: This command does not accept either IP addresses acquired through DHCP or Bootp, or IP addresses that are not configured in a static VLAN on the switch.

Example

If port 3 belongs to a subnetted VLAN that includes an IP address of 10.10.10.100 and you want port 3 to use this secondary address in LLDP advertisements, you need to execute the following command:

```
HP Switch(config)# lldp config 3 ipAddrEnable 10.10.10.100
```

Syntax:

```
[no] lldp config  port-list  basicTlvEnable  TLV-Type
```

port_descr	For outbound LLDP advertisements, this TLV includes an alphanumeric string describing the port. (Default: Enabled)
system_name	For outbound LLDP advertisements, this TLV includes an alphanumeric string showing the assigned name of the system. (Default: Enabled)
system_descr	For outbound LLDP advertisements, this TLV includes an alphanumeric string describing the full name and version identification for the hardware type, software version, and networking application of the system. (Default: Enabled)
system_cap	For outbound advertisements, this TLV includes a bitmask of supported system capabilities (device functions). Also includes information on whether the capabilities are enabled. (Default: Enabled)

Example

If you want to exclude the system name TLV from the outbound LLDP advertisements for all ports on a switch, use this command:

```
HP Switch(config)# no lldp config 1-24 basicTlvEnable system_name
```

If you later decide to reinstate the system name TLV on ports 1-5, use this command:

```
HP Switch(config)# lldp config 1-5 basicTlvEnable system_name
```

Configuring support for port speed and duplex advertisements (CLI)

For more information, see "Support for port speed and duplex advertisements" (page 231).

Syntax:

`[no] lldp config` *`port-list`* `dot3TlvEnable macphy_config`

For outbound advertisements, this TLV includes the (local) switch port's current speed and duplex settings, the range of speed and duplex settings the port supports, and the method required for reconfiguring the speed and duplex settings on the device (autonegotiation during link initialization, or manual configuration).

Using SNMP to compare local and remote information can help in locating configuration mismatches.

(Default: Enabled)

NOTE: For LLDP operation, this TLV is optional. For LLDP-MED operation, this TLV is mandatory.

Configuring the VLAN ID TLV

This TLV advertisement is enabled by default. To enable or disable the TLV, use this command. For more information, see "Port VLAN ID TLV support on LLDP" (page 231).

Syntax:

`[no] lldp config` *`port-list`* `dot1TlvEnable port-vlan-id`

Enables the VLAN ID TLV advertisement.

The `no` form of the command disables the TLV advertisement.

Default: Enabled.

Example

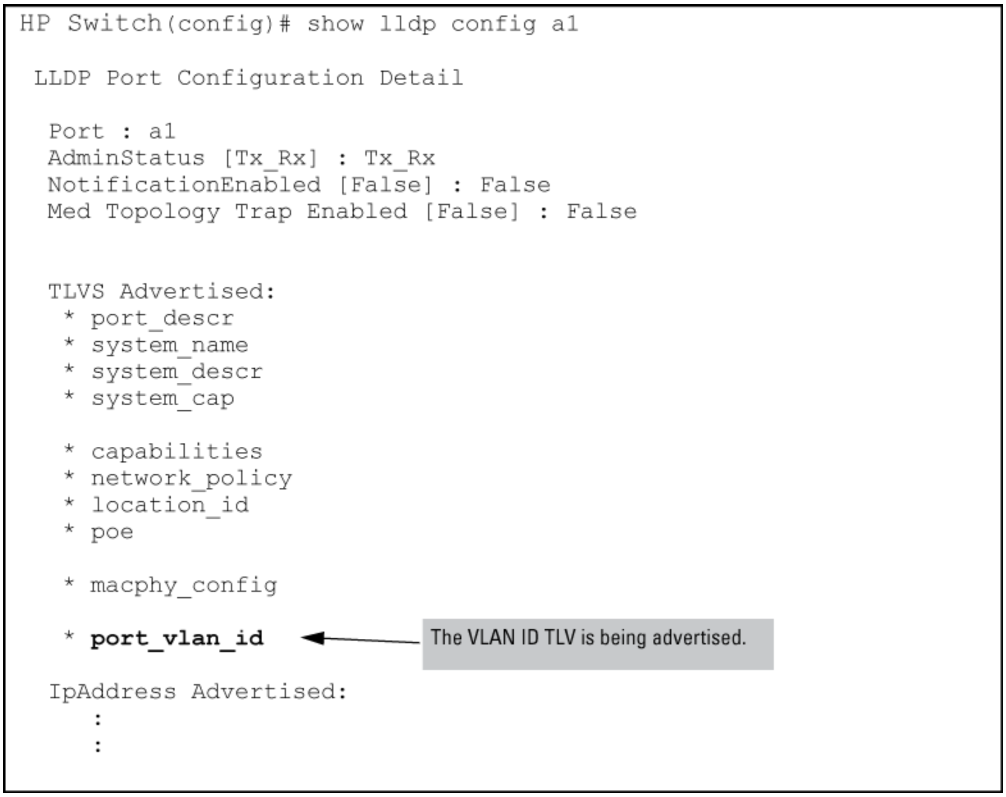
Figure 99 Enabling the VLAN ID TLV

```
HP Switch(config)# lldp config a1 dot1TlvEnable port-vlan-id
```

Viewing the TLVs advertised

The show commands display the configuration of the TLVs. The command `show lldp config` lists the TLVs advertised for each port, as shown in Figure 101 (page 202) through Figure 102 (page 203).

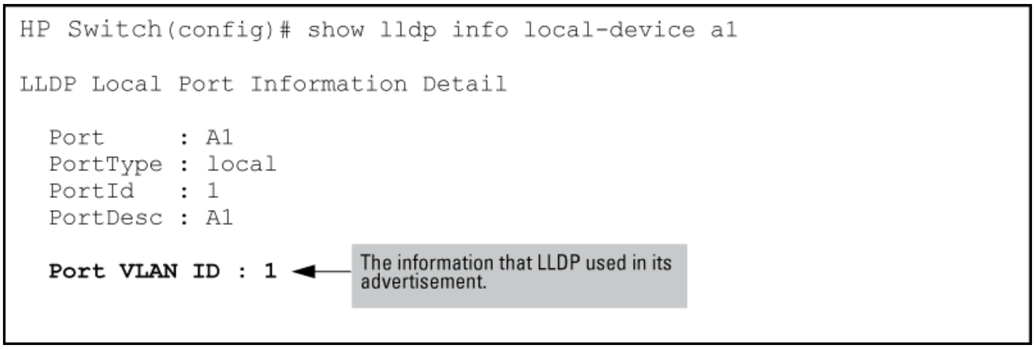
Figure 100 Displaying the TLVs for a port



```
HP Switch(config)# show lldp config a1

 LLDP Port Configuration Detail

  Port : a1
  AdminStatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False


  TLVS Advertised:
   * port_descr
   * system_name
   * system_descr
   * system_cap

   * capabilities
   * network_policy
   * location_id
   * poe

   * macphy_config

   * port_vlan_id

  IpAddress Advertised:
     :
     :
```

The VLAN ID TLV is being advertised.

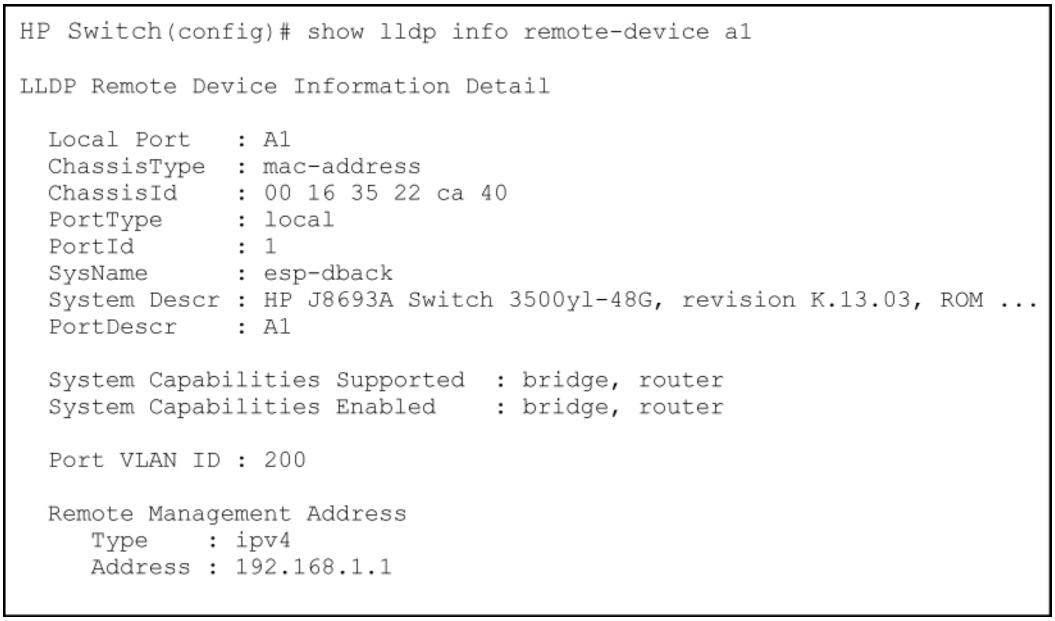
Figure 101 Example of local device LLDP information



```
HP Switch(config)# show lldp info local-device a1

LLDP Local Port Information Detail

  Port     : A1
  PortType : local
  PortId   : 1
  PortDesc : A1

  Port VLAN ID : 1
```

The information that LLDP used in its advertisement.

Figure 102 Example of remote device LLDP information



```
HP Switch(config)# show lldp info remote-device a1

LLDP Remote Device Information Detail

  Local Port    : A1
  ChassisType   : mac-address
  ChassisId     : 00 16 35 22 ca 40
  PortType      : local
  PortId        : 1
  SysName       : esp-dback
  System Descr : HP J8693A Switch 3500yl-48G, revision K.13.03, ROM ...
  PortDescr     : A1

  System Capabilities Supported  : bridge, router
  System Capabilities Enabled    : bridge, router

  Port VLAN ID : 200

  Remote Management Address
     Type     : ipv4
     Address : 192.168.1.1
```

Tracking LLDP-MED connects and disconnects—topology change notification

This optional feature provides information an SNMP application can use to track LLDP-MED connects and disconnects. For more information, see "LLDP-MED (media-endpoint-discovery)" (page 232).

Syntax:

`lldp top-change-notify` *`port-list`*

Topology change notification, when enabled on an LLDP port, causes the switch to send an SNMP trap if it detects LLDP-MED endpoint connection or disconnection activity on the port, or an age-out of the LLDP-MED neighbor on the port. The trap includes the following information:

- The port number (internal) on which the activity was detected (For more on internal port numbers, see "About determining the switch port number included in topology change notification traps" (page 238).)
- The LLDP-MED class of the device detected on the port ("LLDP-MED endpoint device classes" (page 233).)

The `show running` command shows whether the topology change notification feature is enabled or disabled. For example, if ports A1 to A10 have topology change notification enabled, the following entry appears in the `show running` output:

```
lldp top-change-notify A1-A10
```

(Default: Disabled)

NOTE: To send traps, this feature requires access to at least one SNMP server. For information on configuring traps, see "SNMP notifications" (page 221). Also, if a detected LLDP-MED neighbor begins sending advertisements without LLDP-MED TLVs, the switch sends a top-change-notify trap.

LLDP-MED fast start control

Syntax:

```
lldp fast-start-count 1 - 10
```

An LLDP-MED device connecting to a switch port may use the data contained in the MED TLVs from the switch to configure itself. However, the `lldp refresh-interval` setting (default: 30 seconds) for transmitting advertisements can cause an unacceptable delay in MED device configuration.

To support rapid LLDP-MED device configuration, the `lldp fast-start-count` command temporarily overrides the `refresh-interval` setting for the `fast-start-count` advertisement interval. This results in the port initially advertising LLDP-MED at a faster rate for a limited time. Thus, when the switch detects a new LLDP-MED device on a port, it transmits one LLDP-MED advertisement per second out the port for the duration of the `fast-start-count` interval. In most cases, the default setting should provide an adequate `fast-start-count` interval.

(Default: 5 seconds)

NOTE: This global command applies only to ports on which a new LLDP-MED device is detected. It does not override the `refresh-interval` setting on ports where non-MED devices are detected.

Enabling or Disabling medTlvEnable

In the default LLDP-MED configuration, the TLVs controlled by medTlvEnable are enabled. For more information, see "Advertising device capability, network policy, PoE status and location data" (page 234).

Syntax:

```
[no] lldp config  port-list  medTlvEnable  medTlv
```

Enables or disables advertisement of the following TLVs on the specified ports:

- Device capability TLV
- Configured network policy TLV
- Configured location data TLV (see "Configuring location data for LLDP-MED devices" (page 205).)
- Current PoE status TLV

(Default: All of the above TLVs are enabled.)

Helps to locate configuration mismatches by allowing use of an SNMP application to compare the LLDP-MED configuration on a port with the LLDP-MED TLVs advertised by a neighbor connected to that port.

`capabilities`	This TLV enables the switch to determine: • Which LLDP-MED TLVs a connected endpoint can discover • The device class (1, 2, or 3) for the connected endpoint This TLV also enables an LLDP-MED endpoint to discover what LLDP-MED TLVs the switch port currently supports. (Default: enabled) **NOTE:** This TLV cannot be disabled unless the `network_policy`, `poe`, and `location_id` TLVs are already disabled.
`network-policy`	This TLV enables the switch port to advertise its configured network policies (voice VLAN, Layer 2 QoS, Layer 3 QoS), and allows LLDP-MED endpoint devices to autoconfigure the voice network policy advertised by the switch. This also enables the use of SNMP applications to troubleshoot statically configured endpoint network policy mismatches. (Default: Enabled)

	NOTE: Network policy is advertised only for ports that are configured as members of the voice VLAN. If the port belongs to more than one voice VLAN, the voice VLAN with the lowest-numbered VID is selected as the VLAN for voice traffic. Also, this TLV cannot be enabled unless the `capability` TLV is already enabled. For more information, see "Network policy advertisements" (page 234).
`location_id`	This TLV enables the switch port to advertise its configured location data (if any). For more information on configuring location data, see "Configuring location data for LLDP-MED devices" (page 205). (Default: Enabled) **NOTE:** When disabled, this TLV cannot be enabled unless the capability TLV is already enabled.
`poe`	This TLV enables the switch port to advertise its current PoE state and to read the PoE requirements advertised by the LLDP-MED endpoint device connected to the port. (Default: Enabled) **NOTE:** When disabled, this TLV cannot be enabled unless the `capability` TLV is already enabled. For more on this topic, see "PoE advertisements" (page 235)

Viewing PoE advertisements

To display the current power data for an LLDP-MED device connected to a port, use the following command:

```
show lldp info remote-device  port-list
```

For more information on this command, see page A-60.

To display the current PoE configuration on the switch, use the following commands:

```
     show power brief  port-list
     show power  port-list
```

For more information on PoE configuration and operation, see Chapter 11, "Power Over Ethernet (PoE/PoE+) Operation".

Configuring location data for LLDP-MED devices

For more information, see "Location data for LLDP-MED devices" (page 235).

Syntax:

`[no] lldp config` *`port-list`* `medPortLocation` *`Address-Type`*

Configures location of emergency call data the switch advertises per port in the `location_id` TLV. This TLV is for use by LLDP-MED endpoints employing location-based applications.

NOTE: The switch allows one medPortLocation entry per port (without regard to type). Configuring a new medPortLocation entry of any type on a port replaces any previously configured entry on that port.

`civic-addr` *`COUNTRY-STR`* *`WHAT`* *`CA-TYPE`* *`CA-VALUE`* … [*`CA-TYPE`* *`CA-VALUE`*]
… [*`CA-TYPE`* *`CA-VALUE`*]

Enables configuration of a physical address on a switch port and allows up to 75 characters of address information.

`COUNTRY-STR`	A two-character country code, as defined by ISO 3166. Some examples include `FR` (France), `DE` (Germany), and `IN` (India). This field is required in a `civic-addr` command. (For a complete list of country codes, visit **www.iso.org**.)
`WHAT`	A single-digit number specifying the type of device to which the location data applies: **0**: Location of DHCP server **1**: Location of switch **2**: Location of LLDP-MED endpoint (recommended application) This field is required in a `civic-addr` command.

`Type/Value Pairs (CA-TYPE and CA-VALUE)`	A series of data pairs, each composed of a location data "type" specifier and the corresponding location data for that type. That is, the first value in a pair is expected to be the civic address "type" number (`CA-TYPE`), and the second value in a pair is expected to be the corresponding civic address data (`CA-VALUE`). For example, if the `CA-TYPE` for "city name" is "3," the type/value pair to define the city of Paris is "3 Paris." Multiple type/value pairs can be entered in any order, although HP recommends that multiple pairs be entered in ascending order of the `CA-TYPE`. When an emergency call is placed from a properly configured class 3 endpoint device to an appropriate PSAP, the country code, device type, and type/value pairs configured on the switch port are included in the transmission. The "type" specifiers are used by the PSAP to identify and organize the location data components in an understandable format for response personnel to interpret. A `civic-addr` command requires a minimum of one type/value pair, but typically includes multiple type/value pairs as needed to configure a complete set of data describing a given location. `CA-TYPE:` This is the first entry in a type/value pair and is a number defining the type of data contained in the second entry in the type/value pair (`CA-VALUE`). Some examples of `CA-TYPE` specifiers include: • 3=city • 6=street (name) • 25=building name (Range: 0 - 255) For a sample listing of `CA-TYPE` specifiers, see Table 6-5 (page 236). `CA-VALUE:`This is the second entry in a type/value pair and is an alphanumeric string containing the location information corresponding to the immediately preceding `CA-TYPE` entry. Strings are delimited by either blank spaces, single quotes (' … '), or double quotes ("… "). Each string should represent a specific data type in a set of unique type/value pairs comprising the description of a location, and each string must be preceded by a `CA-TYPE` number identifying the type of data in the string. **NOTE:** A switch port allows one instance of any given `CA-TYPE`. For example, if a type/value pair of 6 Atlantic (to specify "Atlantic" as a street name) is configured on port A5 and later another type/value pair of 6 Pacific is configured on the same port, Pacific replaces Atlantic in the civic address location configured for port A5.
`elin-addr emergency-number`	This feature is intended for use in ECS applications to support class 3 LLDP-MED VoIP telephones connected to a switch in an MLTS infrastructure. An ELIN is a valid NANP format telephone number assigned to MLTS operators in North America by the appropriate authority. The ELIN is used to route emergency (E911) calls to a PSAP. (Range: 1-15 numeric characters)

Viewing switch information available for outbound advertisements

Syntax:

`show lldp info local-device [ port-list ]`

Without the `[ port-list ]` option, displays the global switch information and the per-port information currently available for populating outbound LLDP advertisements.

With the `[ port-list ]` option, displays only the following port-specific information that is currently available for outbound LLDP advertisements on the specified ports:

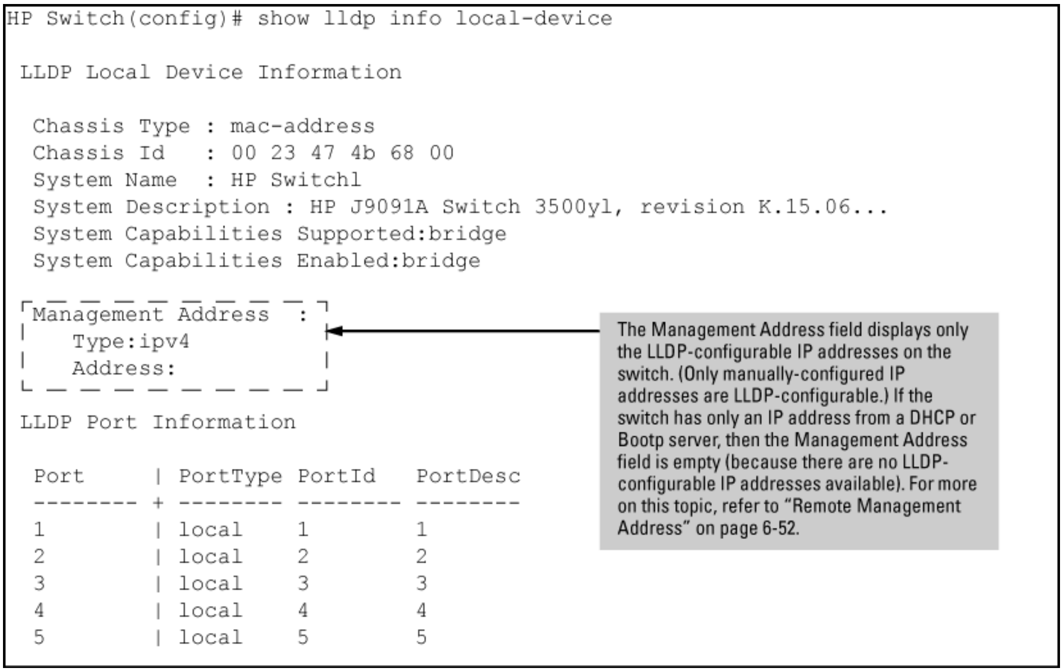
- `PortType`
- `PortId`
- `PortDesc`

NOTE: This command displays the information available on the switch. Use the `lldp config` *`port-list`* command to change the selection of information that is included in actual outbound advertisements. In the default LLDP configuration, all information displayed by this command is transmitted in outbound advertisements.

Example

In the default configuration, the switch information currently available for outbound LLDP advertisements appears similar to the display in Figure 103 (page 208).

Figure 103 Displaying the global and per-port information available for outbound advertisements



```
HP Switch(config)# show lldp info local-device

 LLDP Local Device Information

  Chassis Type : mac-address
  Chassis Id   : 00 23 47 4b 68 00
  System Name  : HP Switch1
  System Description : HP J9091A Switch 3500yl, revision K.15.06...
  System Capabilities Supported:bridge
  System Capabilities Enabled:bridge

  Management Address  :
     Type:ipv4
     Address:

 LLDP Port Information

  Port     | PortType PortId   PortDesc
  -------- + -------- -------- --------
  1        | local    1        1
  2        | local    2        2
  3        | local    3        3
  4        | local    4        4
  5        | local    5        5
```

The Management Address field displays only the LLDP-configurable IP addresses on the switch. (Only manually-configured IP addresses are LLDP-configurable.) If the switch has only an IP address from a DHCP or Bootp server, then the Management Address field is empty (because there are no LLDP-configurable IP addresses available). For more on this topic, refer to "Remote Management Address" on page 6-52.

Figure 104 Example of the default per-port information content for ports 1 and 2

```
HP Switch(config)# show lldp info local 1-2

  LLDP Local Port Information Detail

   Port     : 1
   PortType : local
   PortId   : 1
   PortDesc : 1

----------------------------------------
   Port     : 2
   PortType : local
   PortId   : 2
   PortDesc : 2
```

Viewing the current port speed and duplex configuration on a switch port

For more information, see "About displaying the current port speed and duplex configuration on a switch port" (page 237).

Syntax:

```
show interfaces brief  port-list
```

Includes port speed and duplex configuration in the `Mode` column of the resulting display.

Viewing advertisements currently in the neighbors MIB

Syntax:

```
show lldp info remote-device[ port-list ]
```

Without the `[port-list]` option, provides a global list of the individual devices it has detected by reading LLDP advertisements. Discovered devices are listed by the inbound port on which they were discovered.

Multiple devices listed for a single port indicates that such devices are connected to the switch through a hub.

Discovering the same device on multiple ports indicates that the remote device may be connected to the switch in one of the following ways:

- Through different VLANS using separate links. (This applies to switches that use the same MAC address for all configured VLANs.)
- Through different links in the same trunk.
- Through different links using the same VLAN. (In this case, spanning-tree should be invoked to prevent a network topology loop. Note that LLDP packets travel on links that spanning-tree blocks for other traffic types.)

With the `[port-list]` option, provides a listing of the LLDP data that the switch has detected in advertisements received on the specified ports.

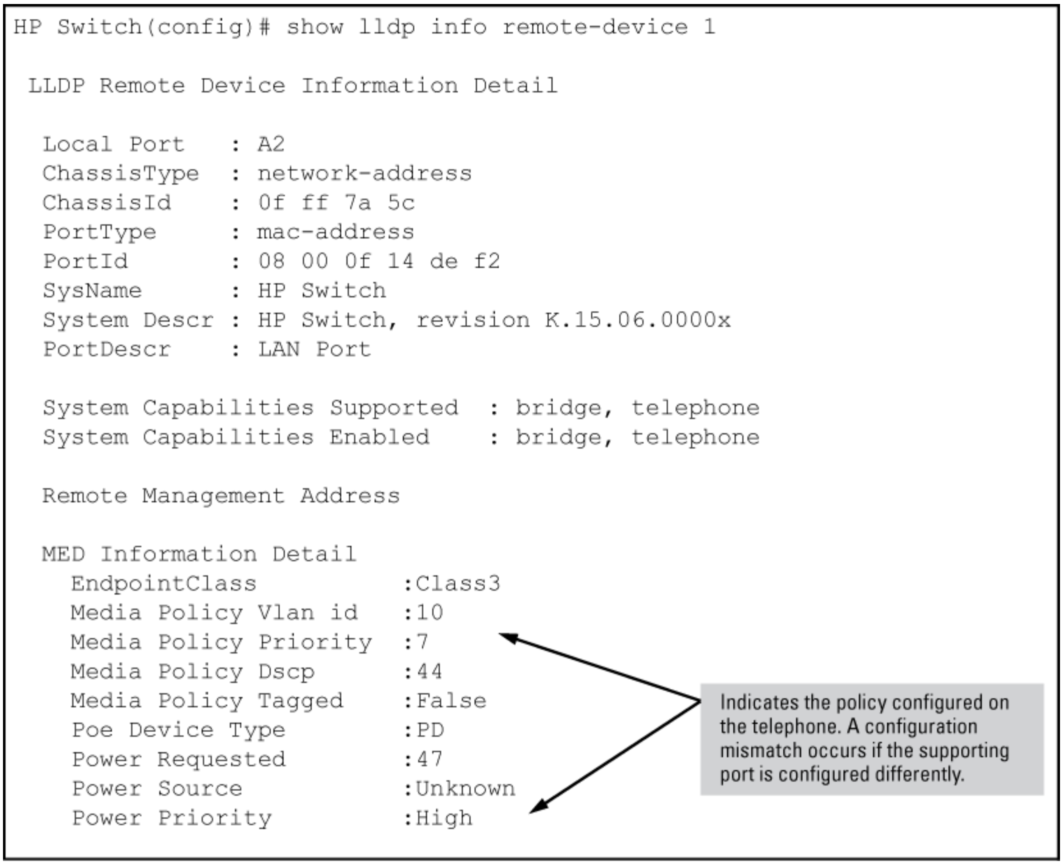
For descriptions of the various types of information displayed by these commands, see Table 6-4 (page 227).

Examples

Example 45 A global listing of discovered devices

```
HP Switch(config)# show lldp info remote

 LLDP Remote Devices Information

  LocalPort | ChassisId                 PortId PortDescr SysName
  --------- + ------------------------- ------ --------- -------------
  1         | 00 11 85 35 3b 80         6      6         HP Switch 3500yl
  2         | 00 11 85 cf 66 60         8      8         HP Switch 3500yl
```

Figure 105 An LLLDP-MED listing of an advertisement received from an LLDP-MED (VoIP telephone) source



```
HP Switch(config)# show lldp info remote-device 1

 LLDP Remote Device Information Detail

  Local Port    : A2
  ChassisType   : network-address
  ChassisId     : 0f ff 7a 5c
  PortType      : mac-address
  PortId        : 08 00 0f 14 de f2
  SysName       : HP Switch
  System Descr : HP Switch, revision K.15.06.0000x
  PortDescr     : LAN Port

  System Capabilities Supported  : bridge, telephone
  System Capabilities Enabled    : bridge, telephone

  Remote Management Address

  MED Information Detail
    EndpointClass          :Class3
    Media Policy Vlan id   :10
    Media Policy Priority  :7
    Media Policy Dscp      :44
    Media Policy Tagged    :False
    Poe Device Type        :PD
    Power Requested        :47
    Power Source           :Unknown
    Power Priority         :High
```

Indicates the policy configured on the telephone. A configuration mismatch occurs if the supporting port is configured differently.

Viewing LLDP statistics

For more information, see "Displaying LLDP statistics" (page 237).

Syntax:

`show lldp stats [ port-list ]`

The *global LLDP* statistics command displays an overview of neighbor detection activity on the switch, plus data on the number of frames sent, received, and discarded per-port.

The *per-port LLDP* statistics command enhances the list of per-port statistics provided by the global statistics command with some additional per-port LLDP statistics.

Global LLDP Counters:

`Neighbor Entries List Last Updated`	The elapsed time since a neighbor was last added or deleted.
`New Neighbor Entries Count`	The total of new LLDP neighbors detected since the last switch reboot. Disconnecting, and then reconnecting a neighbor increments this counter.
`Neighbor Entries Deleted Count`	The number of neighbor deletions from the MIB for AgeOut Count and forced drops for all ports. For example, if the admin status for port on a neighbor device changes from `tx_rx` or `txonly` to `disabled` or `rxonly`, the neighbor device sends a "shutdown" packet out the port and ceases transmitting LLDP frames out that port. The device receiving the shutdown packet deletes all information about the neighbor received on the applicable inbound port and increments the counter.
`Neighbor Entries Dropped Count`	The number of valid LLDP neighbors the switch detected, but could not add. This can occur, for example, when a new neighbor is detected when the switch is already supporting the maximum number of neighbors. See "Neighbor maximum" (page 237).
`Neighbor Entries AgeOut Count`	The number of LLDP neighbors dropped on all ports because of Time-to-Live expiring.

Per-Port LLDP Counters:

`NumFramesRecvd`	The total number of valid, inbound LLDP advertisements received from any neighbors on *`port-list`* . Where multiple neighbors are connected to a port through a hub, this value is the total number of LLDP advertisements received from all sources.
`NumFramesSent`	The total number of LLDP advertisements sent from *`port-list`* .
`NumFramesDiscarded`	The total number of inbound LLDP advertisements discarded by *`port-list`* . This can occur, for example, when a new neighbor is detected on the port, but the switch is already supporting the maximum number of neighbors. See "Neighbor maximum" (page 237). This can also be an indication of advertisement formatting problems in the neighbor device.
`Frames Invalid`	The total number of invalid LLDP advertisements received on the port. An invalid advertisement can be caused by header formatting problems in the neighbor device.
`TLVs Unrecognized`	The total number of LLDP TLVs received on a port with a type value in the reserved range. This can be caused by a basic management TLV from a later LLDP version than the one currently running on the switch.

`TLVs Discarded`	The total number of LLDP TLVs discarded for any reason. In this case, the advertisement carrying the TLV may be accepted, but the individual TLV is not usable.
`Neighbor Ageouts`	The number of LLDP neighbors dropped on the port because of Time-to-Live expiring.

Examples

Example 46 A global LLDP statistics display

```
HP Switch(config)# show lldp stats

 LLDP Device Statistics

  Neighbor Entries List Last Updated : 2 hours
  New Neighbor Entries Count : 20
  Neighbor Entries Deleted Count : 20
  Neighbor Entries Dropped Count : 0
  Neighbor Entries AgeOut Count : 20

 LLDP Port Statistics

  Port   | NumFramesRecvd NumFramesSent NumFramesDiscarded
  ------ + -------------- ------------- ------------------
  A1     | 97317          97843         0
  A2     | 21             12            0
  A3     | 0              0             0
  A4     | 446            252           0
  A5     | 0              0             0
  A6     | 0              0             0
  A7     | 0              0             0
  A8     | 0              0             0
```

Example 47 A per-port LLDP statistics display

```
HP Switch(config)# show lldp stats 1

 LLDP Port Statistics Detail

  PortName : 1
  Frames Discarded  : 0
  Frames Invalid    : 0
  Frames Received   : 7309
  Frames Sent       : 7231
  TLVs Unrecognized : 0
  TLVs Discarded    : 0
  Neighbor Ageouts  : 0
```

Configuring CDP mode

To set the CDP mode to pass-through or receive only, enter this command.

Syntax

```
[no]cdp moden[pass-through | rxonly]
```

Sets the selected mode of CDP processing.

Viewing the current CDP configuration of the switch

CDP is shown as enabled/disabled both globally on the switch and on a per-port basis.

Syntax:

```
show cdp
```

Lists the global and per-port CDP configuration of the switch.

Example

Example 48 Show CDP with the default CDP configuration

This example shows the default CDP configuration.

```
HP Switch(config)# show cdp

 Global CDP information

  Enable CDP [Yes] : Yes (Receive Only)


  Port CDP
  ---- --------
  1    enabled
  2    enabled
  3    enabled
  .      .
  .      .
  .      .
```

Viewing the current CDP neighbors table of the switch

Devices are listed by the port on which they were detected.

Syntax:

```
show cdp neighbors
```

Lists the neighboring CDP devices the switch detects, with a subset of the information collected from the device's CDP packet.

`[ [ e ] port-numb [ detail ] ]`	Lists the CDP device connected to the specified port. (Allows only one port at a time.) Using `detail` provides a longer list of details on the CDP device the switch detects on the specified port.
`[ detail [ [ e ]port-num ] ]`	Provides a list of the details for all of the CDP devices the switch detects. Using `port-num` produces a list of details for the selected port.

Example

Example 49 CDP neighbors table listing

This example displays the CDP devices that the switch has detected by receiving their CDP packets.

```
HP Switch(config)# show cdp neighbors

 CDP neighbors information

  Port Device ID                     | Platform                     Capability
  ---- ----------------------------- + ---------------------------- -----------
  1    Accounting (0030c1-7fcc40)    | J4812A HP Switch. . .        S
  2    Resear¢1-1 (0060b0-889e43)    | J4121A HP Switch. . .        S
  4    Support (0060b0_761a45)       | J4121A HP Switch. . .        S
  7    Marketing (0030c5_33dc59)     | J4313A HP Switch. . .        S
  12   Mgmt NIC(099a05-09df9b        | NIC Model X666               H
  12   Mgmt NIC(099a05-09df11        | NIC Model X666               H
```

Enabling and Disabling CDP Operation

Enabling CDP operation (the default) on the switch causes the switch to add entries to its CDP Neighbors table for any CDP packets it receives from other neighboring CDP devices.

Disabling CDP operation clears the switch's CDP Neighbors table and causes the switch to drop inbound CDP packets from other devices without entering the data in the CDP Neighbors table.

Syntax:

[no] `cdp run`

Enables or disables CDP read-only operation on the switch.

(Default: Enabled)

Example

To disable CDP read-only on the switch:

```
HP Switch(config)# no cdp run
```

When CDP is disabled:

- `show cdp neighbors` displays an empty CDP Neighbors table
- `show cdp` displays
  Global CDP information

  Enable CDP [Yes]: No

Enabling or disabling CDP operation on individual ports

In the factory-default configuration, the switch has all ports enabled to receive CDP packets. Disabling CDP on a port causes it to drop inbound CDP packets without recording their data in the CDP Neighbors table.

Syntax:

[no] `cdp enable` [`[ e ]` *`port-list`*]

Example

To disable CDP on port A1:

```
HP Switch(config)# no cdp enable a1
```

Configuring CDPv2 for voice transmission

Legacy Cisco VOIP phones only support manual configuration or using CDPv2 for voice VLAN auto-configuration. LLDP-MED is not supported. CDPv2 exchanges information such as software version, device capabilities, and voice VLAN information between directly connected devices such as a VOIP phone and a switch.

When the Cisco VOIP phone boots up (or sometimes periodically), it queries the switch and advertises information about itself using CDPv2. The switch receives the VOIP VLAN Query TLV (type 0x0f) from the phone and then immediately sends the voice VLAN ID in a reply packet to the phone using the VLAN Reply TLV (type 0x0e). The phone then begins tagging all packets with the advertised voice VLAN ID.

NOTE: A voice VLAN must be configured before the voice VLAN can be advertised. For example, to configure VLAN 10 as a voice VLAN tagged for ports 1 through 10, enter these commands:

```
HP Switch(config)# vlan 10

HP Switch(vlan-10)# tagged 1-10

HP Switch(vlan-10)# voice

HP Switch(vlan-10)# exit
```

The switch CDP packet includes these TLVs:

- CDP Version: 2
- CDP TTL: 180 seconds
- Checksum
- Capabilities (type 0x04): 0x0008 (is a switch)
- Native VLAN: The PVID of the port
- VOIP VLAN Reply (type 0xe): voice VLAN ID (same as advertised by LLDPMED)
- Trust Bitmap (type 0x12): 0x00
- Untrusted port COS (type 0x13): 0x00

CDP should be enabled and running on the interfaces to which the phones are connected. Use the `cdp enable` and `cdp run` commands.

The `pre-standard-voice` option for the `cdp mode` command allows the configuration of CDP mode so that it responds to received CDP queries from a VoIP phone.

Syntax

```
[no]cdp mode pre-standard-voice [admin-status <port-list>
[tx_rx | rxonly]]
```

Enable CDP-compatible voice VLAN discovery with pre-standard VoIP phones. In this mode, when a CDP VoIP VLAN query is received on a port from pre-standard phones, the switch replies back with a CDP packet that contains the VID of the voice VLAN associated with that port.

NOTE: Not recommended for phones that support LLDP-MED.

pre-standard-voice	Enables CDP-compatible voice VLAN discovery with pre-standard VoIP phones.
admin-status	Sets the port in either transmit and receive mode, or receive mode only. Default: tx-rx.

<port-list>	Sets this port in transmit and receive mode, or receive mode only.
rxonly	Enable receive-only mode of CDP processing.
tx_rx	Enable transmit and receive mode.

```
HP Switch(config)# cdp mode pre-standard-voice admin-status A5 rxonly
```

Show CDP output when CDP Run is disabled

```
HP Switch (config)# show cdp
Global CDP information
Enable CDP [yes] : no
```

show cdp output when cdp run and sdp mode are enabled

```
HP Switch(config)# show cdp
Global CDP Information
Enable CDP [Yes] : Yes
CDP mode [rxonly] : pre-standard-voice
CDP Hold Time [180] : 180
CDP Transmit Interval [60] : 60
Port CDP admin-status
---- --------- ------------
A1   enabled   rxonly
A2   enabled   tx_rx
A3   enabled   tx_rx
```

show cdp output when cdp run and cdp mode rxonly are enabled

When CDP mode is not pre-standard voice, the admin-status column is note displayed.

```
HP Switch(config)# show cdp
Global CDP Information
Enable CDP [Yes} : Yes
CDP mode [rxonly] : rxonly
Port CDP
---- --------
A1   enabled
A2   enabled
A3   enabled
```

show running-config when admin-status is configured

```
HP Switch(config)# show running-config
Running configuration:
; J9477A Configuration Editor; Created on release #K.16.09.0000x
; Ver #03:01:1f:ef:f2
hostname “HPSwitch”
module 1 type J9307A
cdp mode pre-standard-voice admin-status A5 RxOnly
```

Filtering CDP information

In some environments it is desirable to be able to configure a switch to handle CDP packets by filtering out the MAC address learns from untagged VLAN traffic from IP phones. This means that normal protocol processing occurs for the packets, but the addresses associated with these packets is not learned or reported by the software address management components. This enhancement also filters out the MAC address learns from LLDP and 802.1x EAPOL packets on untagged VLANs.

The feature is configured per-port.

Configuring the switch to filter untagged traffic

Enter this command to configure the switch not to learn CDP, LLDP, or EAPOL traffic for a set of interfaces.

Syntax

```
[no]ignore-untagged-mac <port-list>
```

Prevents MAC addresses from being learned on the specified ports when the VLAN is untagged and the destination MAC address is one of the following:

- 01000C-CCCCCC (CDP)
- 0180c2- 00000e (LLDP)
- 0180c2-000003 (EAPOL)

Configuring the switch to ignore packet MAC address learns for an untagged VLAN

```
HP Switch(config) ignore-untagged-mac 1-2
```

Displaying the configuration

Enter the `show running-config` command to display information about the configuration.

Configuration showing interfaces to ignore packet MAC address learns

```
HP Switch(config) show running-config
Running configuration:
; J9627 Configuration Editor; Created on release K.15.XX
; Ver #03:03.1f.ef:f0
hostname “HP Switch”
interface 1
ignore-untagged-mac
exit
interface 2
ignore-untagged-mac
exit
...
vlan 1
name “DEFAULT_VLAN”
untagged 1-24
ip address dhcp-bootp
exit
```

About using SNMP tools to manage the switch

SNMP is a management protocol that allows an SNMP client application to retrieve device configuration and status information and to configure the device (*get* and *set*). You can manage the switch via SNMP from a network management station running an application such as PCM+. For more information on PCM+, see the HP website at:

www.hp.com/networking

From the **Products** menu, select **Network Management**. The click on **PCM+ Network Management** under the **HP Network Management** bar.

To implement SNMP management, the switch must have an IP address configured either manually or dynamically (using DHCP or Bootp). If multiple VLANs are configured, each VLAN interface should have its own IP address. For DHCP use with multiple VLANs, see section "The Primary VLAN" in the "Static Virtual LANs (VLANs)" chapter of the *Advanced Traffic Management Guide* for your switch.

NOTE: If you use the switch's Authorized IP Managers and Management VLAN features, ensure that the SNMP management station, the choice of switch port used for SNMP access to the switch, or both, are compatible with the access controls enforced by these features. Otherwise, SNMP access to the switch will be blocked.

For more information on Authorized IP Managers, see the *Access Security Guide* for your switch. (The latest version of this guide is available on the HP Networking website.) For information on the Management VLAN feature, see the section "The Secure Management VLAN" in the "Static Virtual LANs (VLANs)" chapter of the *Advanced Traffic Management Guide* for your switch.

SNMP management features

SNMP management features on the switch include:

- SNMP version 1, version 2c, or version 3 over IP
- Security via configuration of SNMP communities ("SNMPv3 communities" (page 221))
- Security via authentication and privacy for SNMPv3 access
- Event reporting via SNMP
  - Version 1 traps
  - RMON: groups 1, 2, 3, and 9
- PCM/PCM+
- Flow sampling using sFlow
- Standard MIBs, such as the Bridge MIB (RFC 1493), Ethernet MAU MIB (RFC 1515), and others.

The switch SNMP agent also uses certain variables that are included in an HP proprietary MIB (management information base) file. If you are using HP OpenView, you can ensure that it is using the latest version of the MIB file by downloading the file to the OpenView database. To do so, go to the HP Networking website at:

www.hp.com/Networking/support

1. Type a model number of your switch (for example, 8212) or product number in the **Auto Search** text box.
2. Select an appropriate product from the drop down list.
3. Click the Display selected button.
4. From the options that appear, select Software downloads.
5. MIBs are available with switch software in the Other category.

Click on `software updates`, then `MIBs`.

SNMPv1 and v2c access to the switch

SNMP access requires an IP address and subnet mask configured on the switch. If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address.

Once an IP address is configured, the main steps for configuring SNMPv1 and v2c access management features are:

1. Configure the appropriate SNMP communities. (See "SNMPv3 communities" (page 221).)
2. Configure the appropriate trap receivers. (See "SNMP notifications" (page 221).)

In some networks, authorized IP manager addresses are not used. In this case, all management stations using the correct community name may access the switch with the View and Access levels that have been set for that community. If you want to restrict access to one or more specific nodes, you can use the switch's IP Authorized Manager feature. (See the *Access Security Guide* for your switch.)

△ **CAUTION:** For PCM/PCM+ version 1.5 or earlier (or any TopTools version), deleting the "public" community disables some network management functions (such as traffic monitoring, SNMP trap generation, and threshold setting). If network management security is a concern, and you are using the above software versions, HP recommends that you change the write access for the "public" community to "Restricted."

SNMPv3 access to the switch

SNMPv3 access requires an IP address and subnet mask configured on the switch. (See "IP Configuration" on page 8-2.) If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address. (See "DHCP/Bootp Operation".)

Once you have configured an IP address, the main steps for configuring SNMPv3 access management features are the following:

1. Enable SNMPv3 for operation on the switch (see "Enabling SNMPv3" (page 172)).
2. Configure the appropriate SNMP users (see "SNMPv3 users" (page 219)).
3. Configure the appropriate SNMP communities (see "SNMPv3 communities" (page 221)).
4. Configure the appropriate trap receivers (see "SNMP notifications" (page 221)).

In some networks, authorized IP manager addresses are not used. In this case, all management stations using the correct User and community name may access the switch with the View and Access levels that have been set for that community. If you want to restrict access to one or more specific nodes, you can use the IP Authorized Manager feature for the switch. (See the *Access Security Guide* for your switch.)

SNMP version 3 (SNMPv3) adds some new commands to the CLI for configuring SNMPv3 functions. To enable SNMMPv3 operation on the switch, use the `snmpv3 enable` command. An initial user entry will be generated with MD5 authentication and DES privacy.

You may (optionally) restrict access to only SNMPv3 agents by using the `snmpv3 only` command. To restrict write-access to only SNMPv3 agents, use the `snmpv3 restricted-access` command.

△ **CAUTION:** Restricting access to only version 3 messages will make the community named "public" inaccessible to network management applications (such as autodiscovery, traffic monitoring, SNMP trap generation, and threshold setting) from operating in the switch.

SNMPv3 users

NOTE: To create new users, most SNMPv3 management software requires an initial user record to clone. The initial user record can be downgraded and provided with fewer features, but not upgraded by adding new features. For this reason, HP recommends that when you enable SNMPv3, you also create a second user with SHA authentication and DES privacy.

To use SNMPv3 on the switch, you must configure the users that will be assigned to different groups:

1. Configure users in the User Table with the `snmpv3 user` command.
   To view the list of configured users, enter the `show snmpv3 user` command (see "About adding users" (page 220)).

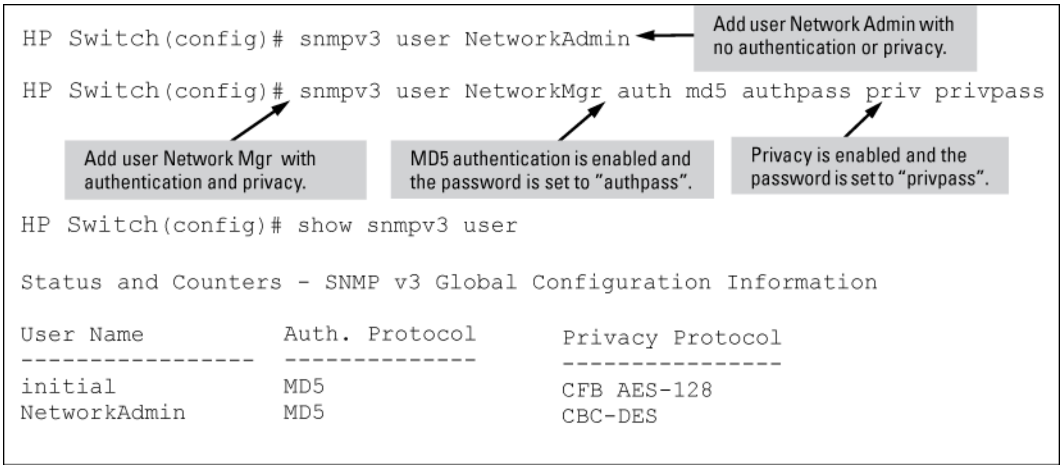
2. Assign users to Security Groups based on their security model with the `snmpv3 group` command (see "Assigning users to groups (CLI)" (page 174)).

△ **CAUTION:** If you add an SNMPv3 user without authentication, privacy, or both, to a group that requires either feature, the user will not be able to access the switch. Ensure that you add a user with the appropriate security level to an existing security group.

About adding users

To configure an SNMPv3 user, you must first add the user name to the list of known users with the `snmpv3 user` command, as shown in Figure 106 (page 220).

Figure 106 Adding SNMPv3 users and displaying SNMPv3 configuration



```
HP Switch(config)# snmpv3 user NetworkAdmin

HP Switch(config)# snmpv3 user NetworkMgr auth md5 authpass priv privpass

HP Switch(config)# show snmpv3 user

Status and Counters - SNMP v3 Global Configuration Information

User Name          Auth. Protocol     Privacy Protocol
-----------------  --------------     ----------------
initial            MD5                CFB AES-128
NetworkAdmin       MD5                CBC-DES
```

Add user Network Admin with no authentication or privacy.

Add user Network Mgr with authentication and privacy.

MD5 authentication is enabled and the password is set to "authpass".

Privacy is enabled and the password is set to "privpass".

Group access levels

The switch supports eight predefined group access levels, shown in Table 6-3 (page 220). There are four levels for use by version 3 users and four are used for access by version 2c or version 1 management applications.

Table 24 Predefined group access levels

Group name	Group access type	Group read view	Group write view
managerpriv	Ver3 Must have Authentication and Privacy	ManagerReadView	ManagerWriteView
managerauth	Ver3 Must have Authentication	ManagerReadView	ManagerWriteView
operatorauth	Ver3 Must have Authentication	OperatorReadView	DiscoveryView
operatornoauth	Ver3 No Authentication	OperatorReadView	DiscoveryView
commanagerrw	Ver2c or Ver1	ManagerReadView	ManagerWriteView
commanagerr	Ver2c or Ver1	ManagerReadView	DiscoveryView
comoperatorrw	Ver2c or Ver1	OperatorReadView	OperatorReadView
comoperatorr	Ver2c or Ver1	OperatorReadView	DiscoveryView

Each view allows you to view or modify a different set of MIBs:

- **Manager Read View** – access to all managed objects
- **Manager Write View** – access to all managed objects except the following:
  - vacmContextTable
  - vacmAccessTable
  - vacmViewTreeFamilyTable
- **OperatorReadView** – no access to the following:
  - icfSecurityMIB
  - hpSwitchIpTftpMode

  - vacmContextTable
  - vacmAccessTable
  - vacmViewTreeFamilyTable
  - usmUserTable
  - snmpCommunityTable
- **Discovery View** – Access limited to samplingProbe MIB.

NOTE: All access groups and views are predefined on the switch. There is no method to modify or add groups or views to those that are predefined on the switch.

SNMPv3 communities

SNMP commuities are supported by the switch to allow management applications that use version 2c or version 1 to access the switch. The communities are mapped to Group Access Levels that are used for version 2c or version 1 support. This mapping happens automatically based on the communities access privileges, but special mappings can be added with the `snmpv3 community` command (see "Mapping SNMPv3 communities (CLI)" (page 175)).

SNMP community features

Use SNMP communities to restrict access to the switch by SNMP management stations by adding, editing, or deleting SNMP communities. You can configure up to five SNMP communities, each with either an operator-level or a manager-level view and either restricted or unrestricted write access.

Using SNMP requires that the switch have an IP address and subnet mask compatible with your network.

△ **CAUTION:** For PCM/PCM+ version 1.5 or earlier (or any TopTools version), deleting the "public" community disables some network management functions (such as traffic monitoring, SNMP trap generation, and threshold setting). If network management security is a concern, and if you are using the above software versions, HP recommends that you change the write access for the "public" community to "Restricted."

SNMP notifications

The switches:

- Fixed or "Well-Known" Traps: A switch automatically sends fixed traps (such as "coldStart", "warmStart", "linkDown", and "linkUp") to trap receivers using the public community name, which is the default. These traps can also be sent to non-public communities.
- SNMPv2c informs
- SNMP v3 notification process, including traps

This section describes how to configure a switch to send network security and link-change notifications to configured trap receivers.

Supported Notifications

By default, the following notifications are enabled on a switch:

- Manager password changes
- SNMP authentication failure
- Link-change traps: when the link on a port changes from up to down (linkDown) or down to up (linkUp)

- Port-security (web, MAC, or 802.1X) authentication failure
- Invalid password entered in a login attempt through a direct serial, Telnet, or SSH connection
- Inability to establish a connection with the RADIUS or TACACS+ authentication server
- DHCP snooping events
- ARP protection events

General steps for configuring SNMP notifications

1. Determine the versions of SNMP notifications that you want to use in your network.

   If you want to use SNMPv1 and SNMPv2c traps, you must also configure a trap receiver. See the following sections and follow the required configuration procedures:

   - "SNMPv1 and SNMPv2c Traps" (page 222)
   - "Configuring an SNMP trap receiver (CLI)" (page 178)
   - "Enabling SNMPv2c informs (CLI)" (page 179)

   If you want to use SNMPv3 notifications (including traps), you must also configure an SNMPv3 management station. Follow the required configuration procedure in "Configuring SNMPv3 notifications (CLI)" (page 180).

2. To reconfigure any of the SNMP notifications that are enabled by default to be sent to a management station (trap receiver), see "Enabling Link-Change Traps (CLI)" (page 184).
3. (Optional) See the following sections to configure optional SNMP notification features and verify the current configuration:
   - "Configuring the source IP address for SNMP notifications (CLI)" (page 187)
   - "Viewing SNMP notification configuration (CLI)" (page 188)

SNMPv1 and SNMPv2c Traps

The switches support the following functionality from earlier SNMP versions (SNMPv1 and SNMPv2c):

- **Trap receivers**: A *trap receiver* is a management station to which the switch sends SNMP traps and (optionally) event log messages sent from the switch. From the CLI you can configure up to ten SNMP trap receivers to receive SNMP traps from the switch.
- **Fixed or "Well-Known" Traps**: A switch automatically sends fixed traps (such as "coldStart", "warmStart", "linkDown", and "linkUp") to trap receivers using the `public` community name. These traps cannot be redirected to other communities. If you change or delete the default `public` community name, these traps are not sent.
- **Thresholds**: A switch automatically sends all messages created when a system threshold is reached to the network management station that configured the threshold, regardless of the trap receiver configuration.

SNMP trap receivers

Use the `snmp-server host` command to configure a trap receiver that can receive SNMPv1 and SNMPv2c traps, and (optionally) Event Log messages. When you configure a trap receiver, you specify its community membership, management station IP address, and (optionally) the type of Event Log messages to be sent.

If you specify a community name that does not exist—that is, has not yet been configured on the switch—the switch still accepts the trap receiver assignment. However, no traps are sent to that trap receiver until the community to which it belongs has been configured on the switch.

NOTE: To replace one community name with another for the same IP address, you must first enter the
`no snmp-server host` *`community-name`* *`ipv4-address`* `|` *`ipv6-address`*
command to delete the unwanted community name. Otherwise, if you add a new community name with an IP address that is already used with a different community name, two valid community name entries are created for the same management station.

If you do not specify the event level (`[ none | all | not-info | critical | debug ]`), the switch does not send Event Log messages as traps. However, "well-known" traps and threshold traps (if configured) are still sent.

About configuring SNMP notification support

You can enable SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices, and control the interval between successive notifications of data changes on the same neighbor.

SNMPv2c informs

On a switch enabled for SNMPv2c, you can use the `snmp-server host inform` command (“Enabling SNMPv2c informs (CLI)” (page 179)) to send inform requests when certain events occur. When an SNMP Manager receives an inform request, it can send an SNMP response back to the sending agent on the switch to let the agent know that the inform request reached its destination.

If the sending agent on the switch does not receive an SNMP response back from the SNMP Manager within the timeout period, the inform request may be resent, based on the retry count value.

When you enable SNMPv2c inform requests to be sent, you must specify the IP address and community name of the management station that will receive the inform notification.

Network security notifications

By default, a switch is enabled to send the SNMP notifications listed in “Supported Notifications” (page 221) when a network security event (for example, authentication failure) occurs. However, before security notifications can be sent, you must first configure one or more trap receivers or SNMPv3 management stations as described in:

- “Configuring an SNMP trap receiver (CLI)” (page 178)
- “Configuring SNMPv3 notifications (CLI)” (page 180)

You can manage the default configuration of the switch to disable and re-enable notifications to be sent for the following types of security events:

- ARP protection events
- Inability to establish a connection with the RADIUS or TACACS+ authentication server
- DHCP snooping events
- Dynamic IP Lockdown hardware resources consumed
- Link change notification
- Invalid password entered in a login attempt through a direct serial, Telnet, or SSH connection
- Manager password changes
- Port-security (web, MAC, or802.1X) authentication failure
- SNMP authentication failure
- Running configuration changes

SNMP traps on running configuration changes

You can send a specific SNMP trap for any configuration change made in the switch's running configuration file. The trap will be generated for changes made from any of these interfaces:

- CLI
- Menu
- SNMP (remote SNMP set requests).

The SNMP trap contains the following information.

Information	Description
Event ID	An assigned number that identifies a specific running configuration change event.
Method	Method by which the change was made—CLI, Menu, or remote SNMP. For configuration changes triggered by internal events, the term "Internal-Event" is used as the source of the change.
IP Address Type	Indicates the source address type of the network agent that made a change. This is set to an address type of "unknown" when not applicable.
IP address	IP address of the remote system from which a user accessed the switch. If not applicable, this is an empty string and nothing is displayed, for example, if access is through a management console port.
User Name	User name of the person who made the change. Null if not applicable.
Date and Time	Date and time the change was made.

The SNMP trap alerts any interested parties that someone has changed the switch's configuration and provides information about the source for that change. It does not specify what has been changed.

Source IP address for SNMP notifications

The switch uses an interface IP address as the source IP address in IP headers when sending SNMP notifications (traps and informs) or responses to SNMP requests.

For multi-netted interfaces, the source IP address is the IP address of the outbound interface of the SNMP reply, which may differ from the destination IP address in the IP header of the received request. For security reasons, it may be desirable to send an SNMP reply with the IP address of the destination interface (or a specified IP address) on which the corresponding SNMP request was received.

To configure the switch to use the source IP address on which an SNMP request was received in SNMP notification/traps and replies, enter the `snmp-server response-source` ((page 187)) and `snmp-server trap-source` ((page 187)) commands.

Listening mode

For switches that have a separate out-of-band management port, you can specify whether a configured SNMP server listens for SNMP queries over the OOBM interface, the data interface, or both. By default, the switch listens over both interfaces.

This option is not available for switches that do not have a separate OOBM port. For more information on network OOBM, see Appendix I, "Network Out-of-Band Management (OOBM)" in this guide.

The listening mode is set with parameters to the `snmp-server` command.

Advanced management: RMON

The switch supports RMON (remote monitoring) on all connected network segments. This allows for troubleshooting and optimizing your network.

The following RMON groups are supported:

- Ethernet Statistics (except the numbers of packets of different frame sizes)
- Alarm
- History (of the supported Ethernet statistics)
- Event

The RMON agent automatically runs in the switch. Use the RMON management station on your network to enable or disable specific RMON traps and events. Note that you can access the Ethernet statistics, Alarm, and Event groups from the HP Switch Manager network management software. For more information on PCM+, see the HP Networking web site at

> www.hp.com/networking
>
> From the Products menu, select Network Management. Then click on PCM+ Network Management under the HP Network Management bar.

CLI-configured sFlow with multiple instances

In earlier software releases, sFlow was configured on the switch via SNMP using a single sFlow instance. Beginning with software release K.11.34, sFlow can also be configured via the CLI for up to three distinct sFlow instances: once enabled, an sFlow receiver/destination can be independently configured for full flow-sampling and counter-polling. CLI-configured sFlow instances may be saved to the startup configuration to persist across a switch reboot.

LLDP

To standardize device discovery on all HP switches, LLDP will be implemented while offering limited read-only support for CDP, as documented in this manual. For the latest information on your switch model, consult the Release Notes (available on the HP Networking website). If LLDP has not yet been implemented (or if you are running an older version of software), consult a previous version of the *Management and Configuration Guide* for device discovery details.

LLDP (Link Layer Discovery Protocol): provides a standards-based method for enabling the switches covered in this guide to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

LLDP-MED (LLDP Media Endpoint Discovery): Provides an extension to LLDP and is designed to support VoIP deployments.

NOTE: LLDP-MED is an extension for LLDP, and the switch requires that LLDP be enabled as a prerequisite to LLDP-MED operation.

An SNMP utility can progressively discover LLDP devices in a network by:

1. Reading a given device's Neighbors table (in the Management Information Base, or MIB) to learn about other, neighboring LLDP devices.
2. Using the information learned in step 1 to find and read the neighbor devices' Neighbors tables to learn about additional devices, and so on.

Also, by using `show` commands to access the switch's neighbor database for information collected by an individual switch, system administrators can learn about other devices connected to the switch, including device type (capability) and some configuration information. In VoIP deployments using LLDP-MED on the switches, additional support unique to VoIP applications is also available. See “LLDP-MED (media-endpoint-discovery)” (page 232).

General LLDP operation

An LLDP packet contains data about the transmitting switch and port. The switch advertises itself to adjacent (neighbor) devices by transmitting LLDP data packets out all ports on which outbound LLDP is enabled and by reading LLDP advertisements from neighbor devices on ports that are inbound LLDP-enabled. (LLDP is a one-way protocol and does not include any acknowledgement mechanism.) An LLDP-enabled port receiving LLDP packets inbound from neighbor devices stores the packet data in a Neighbor database (MIB).

LLDP-MED

This capability is an extension to LLDP and is available on the switches. See "LLDP-MED (media-endpoint-discovery)" (page 232).

Packet boundaries in a network topology

- Where multiple LLDP devices are directly connected, an outbound LLDP packet travels only to the next LLDP device. An LLDP-capable device does not forward LLDP packets to any other devices, regardless of whether they are LLDP-enabled.
- An intervening hub or repeater forwards the LLDP packets it receives in the same manner as any other multicast packets it receives. Thus, two LLDP switches joined by a hub or repeater handle LLDP traffic in the same way that they would if directly connected.
- Any intervening 802.1D device or Layer-3 device that is either LLDP-unaware or has disabled LLDP operation drops the packet.

LLDP operation configuration options

In the default configuration, LLDP is enabled and in both transmit and receive mode on all active ports. The LLDP configuration includes global settings, which apply to all active ports on the switch, and per-port settings, which affect only the operation of the specified ports.

The commands in the LLDP sections affect both LLDP and LLDP-MED operation. For information on operation and configuration unique to LLDP-MED, see "LLDP-MED (media-endpoint-discovery)" (page 232).

Enable or disable LLDP on the switch

In the default configuration, LLDP is globally enabled on the switch. To prevent transmission or receipt of LLDP traffic, you can disable LLDP operation (see syntax (page 196)).

Enable or disable LLDP-MED

In the default configuration for the switches, LLDP-MED is enabled by default. (Requires that LLDP is also enabled.) For more information, see "LLDP-MED (media-endpoint-discovery)" (page 232).

Change the frequency of LLDP packet transmission to neighbor devices

On a global basis, you can increase or decrease the frequency of outbound LLDP advertisements (see syntax (page 197)).

Change the Time-To-Live for LLDP packets sent to neighbors

On a global basis, you can increase or decrease the time that the information in an LLDP packet outbound from the switch will be maintained in a neighbor LLDP device (see syntax (page 197)).

Transmit and receive mode

With LLDP enabled, the switch periodically transmits an LLDP advertisement (packet) out each active port enabled for outbound LLDP transmissions and receives LLDP advertisements on each active port enabled to receive LLDP traffic (Section (page 199)). Per-port configuration options include four modes:

- Transmit and receive (`tx_rx`): This is the default setting on all ports. It enables a given port to both transmit and receive LLDP packets and to store the data from received (inbound) LLDP packets in the switch's MIB.
- Transmit only (`txonly`): This setting enables a port to transmit LLDP packets that can be read by LLDP neighbors. However, the port drops inbound LLDP packets from LLDP neighbors without reading them. This prevents the switch from learning about LLDP neighbors on that port.
- Receive only (`rxonly`): This setting enables a port to receive and read LLDP packets from LLDP neighbors and to store the packet data in the switch's MIB. However, the port does not transmit outbound LLDP packets. This prevents LLDP neighbors from learning about the switch through that port.
- Disable (`disable`): This setting disables LLDP packet transmissions and reception on a port. In this state, the switch does not use the port for either learning about LLDP neighbors or informing LLDP neighbors of its presence.

SNMP notification

You can enable the switch to send a notification to any configured SNMP trap receiver(s) when the switch detects a remote LLDP data change on an LLDP-enabled port (SNMP notification support (page 230)).

Per-port (outbound) data options

The following table lists the information the switch can include in the per-port, outbound LLDP packets it generates. In the default configuration, all outbound LLDP packets include this information in the TLVs transmitted to neighbor devices. However, you can configure LLDP advertisements on a per-port basis to omit some of this information (Section (page 200)).

Table 25 Data available for basic LLDP advertisements

Data type	Configuration options	Default	Description
Time-to-Live	[1].	120 Seconds	The length of time an LLDP neighbor retains the advertised data before discarding it.
Chassis Type[2, 3]	N/A	Always Enabled	Indicates the type of identifier used for Chassis ID.
Chassis ID[3]	N/A	Always Enabled	Uses base MAC address of the switch.
Port Type[4, 3]	N/A	Always Enabled	Uses "Local," meaning assigned locally by LLDP.
Port Id[3]	N/A	Always Enabled	Uses port number of the physical port. This is an internal number reflecting the reserved slot/port position in the chassis. For more information on this numbering scheme, see figures D-2 and D-3 in Appendix D, "MAC Address Management" of the *Management and Configuration Guide* for your switch.

Table 25 Data available for basic LLDP advertisements *(continued)*

Data type	Configuration options	Default	Description
Remote Management Address			
Type[5, 3]	N/A	Always Enabled	Shows the network address type.
Address[5]	Default or Configured	Uses a default address selection method unless an optional address is configured. See "Remote management address" (page 228).	
System Name[3]	Enable/Disable	Enabled	Uses the switch's assigned name.
System Description[3]	Enable/Disable	Enabled	Includes switch model name and running software version, and ROM version.
Port Description[3]	Enable/Disable	Enabled	Uses the physical port identifier.
System capabilities supported[6, 3]	Enable/Disable	Enabled	Identifies the switch's primary capabilities (bridge, router).
System capabilities enabled[6, 3]	Enable/Disable	Enabled	Identifies the primary switch functions that are enabled, such as routing.

[1] The Packet Time-to-Live value is included in LLDP data packets. (See "Changing the time-to-live for transmitted advertisements (CLI)" (page 197).)

[2] Subelement of the Chassis ID TLV.

[3] Populated with data captured internally by the switch. For more on these data types, refer to the IEEE P802.1AB Standard.

[4] Subelement of the Port ID TLV.

[5] Subelement of the Remote-Management-Address TLV.

[6] Subelement of the System Capability TLV.

Remote management address

The switch always includes an IP address in its LLDP advertisements. This can be either an address selected by a default process or an address configured for inclusion in advertisements. See "IP address advertisements" (page 229).

Debug logging

You can enable LLDP debug logging to a configured debug destination (Syslog server, a terminal device, or both) by executing the `debug lldp` command. (For more information on Debug and Syslog, see the "Troubleshooting" appendix in this guide.) Note that the switch's Event Log does not record usual LLDP update messages.

Options for reading LLDP information collected by the switch

You can extract LLDP information from the switch to identify adjacent LLDP devices. Options include:

- Using the switch's `show lldp info` command options to display data collected on adjacent LLDP devices—as well as the local data the switch is transmitting to adjacent LLDP devices ("Displaying the global LLDP, port admin, and SNMP notification status (CLI)" (page 195)).
- Using an SNMP application that is designed to query the Neighbors MIB for LLDP data to use in device discovery and topology mapping.
- Using the `walkmib` command to display a listing of the LLDP MIB objects

LLDP and LLDP-MED standards compatibility

The operation covered by this section is compatible with these standards:

- IEEE P802.1AB
- RFC 2922 (PTOPO, or Physical Topology MIB)
- RFC 2737 (Entity MIB)
- RFC 2863 (Interfaces MIB)
- ANSI/TIA-1057/D6 (LLDP-MED; refer to “LLDP-MED (media-endpoint-discovery)” (page 232).)

LLDP operating rules

For additional information specific to LLDP-MED operation, see “LLDP-MED (media-endpoint-discovery)” (page 232).

Port trunking

LLDP manages trunked ports individually. That is, trunked ports are configured individually for LLDP operation, in the same manner as non-trunked ports. Also, LLDP sends separate advertisements on each port in a trunk, and not on a per-trunk basis. Similarly, LLDP data received through trunked ports is stored individually, per-port.

IP address advertisements

In the default operation, if a port belongs to only one static VLAN, the port advertises the lowest-order IP address configured on that VLAN. If a port belongs to multiple VLANs, the port advertises the lowest-order IP address configured on the VLAN with the lowest VID. If the qualifying VLAN does not have an IP address, the port advertises 127.0.0.1 as its IP address. For example, if the port is a member of the default VLAN (VID=1), and there is an IP address configured for the default VLAN, the port advertises this IP address. In the default operation, the IP address that LLDP uses can be an address acquired by DHCP or Bootp.

You can override the default operation by configuring the port to advertise any IP address that is manually configured on the switch, even if the port does not belong to the VLAN configured with the selected IP address (Section (page 200)). (Note that LLDP cannot be configured through the CLI to advertise an addresses acquired through DHCP or Bootp. However, as mentioned above, in the default LLDP configuration, if the lowest-order IP address on the VLAN with the lowest VID for a given port is a DHCP or Bootp address, the switch includes this address in its LLDP advertisements unless another address is configured for advertisements on that port.) Also, although LLDP allows configuring multiple remote management addresses on a port, only the lowest-order address configured on the port will be included in outbound advertisements. Attempting to use the CLI to configure LLDP with an IP address that is either not configured on a VLAN or has been acquired by DHCP or Bootp results in the following error message.

```
xxx.xxx.xxx.xxx: This IP address is not configured or is a DHCP address.
```

Spanning-tree blocking

Spanning tree does not prevent LLDP packet transmission or receipt on STP-blocked links.

802.1X blocking

Ports blocked by 802.1X operation do not allow transmission or receipt of LLDP packets.

LLDP operation on the switch

Enabling LLDP operation (the default) causes the switch to:

- Use active, LLDP-enabled ports to transmit LLDP packets describing itself to neighbor devices.
- Add entries to its neighbors table based on data read from incoming LLDP advertisements.

Time-to-Live for transmitted advertisements

The Time-to-Live value (in seconds) for all LLDP advertisements transmitted from a switch is controlled by the switch that generates the advertisement and determines how long an LLDP neighbor retains the advertised data before discarding it. The Time-to-Live value is the result of multiplying the `refresh-interval` by the `holdtime-multiplier`.

Delay interval between advertisements generated by value or status changes to the LLDP MIB

The switch uses a *delay-interval* setting to delay transmitting successive advertisements resulting from these LLDP MIB changes. If a switch is subject to frequent changes to its LLDP MIB, lengthening this interval can reduce the frequency of successive advertisements. You can change the delay-interval by using either an SNMP network management application or the CLI `setmib` command.

Reinitialization delay interval

In the default configuration, a port receiving a `disable` command followed immediately by a `txonly`, `rxonly`, or `tx_rx` command delays reinitializing for two seconds, during which LLDP operation remains disabled. If an active port is subjected to frequent toggling between the LLDP disabled and enabled states, LLDP advertisements are more frequently transmitted to the neighbor device. Also, the neighbor table in the adjacent device changes more frequently as it deletes, then replaces LLDP data for the affected port which, in turn, generates SNMP traps (if trap receivers and SNMP notification are configured). All of this can unnecessarily increase network traffic. Extending the reinitialization-delay interval delays the ability of the port to reinitialize and generate LLDP traffic following an LLDP disable/enable cycle.

SNMP notification support

You can enable SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices and control the interval between successive notifications of data changes on the same neighbor.

Changing the minimum interval for successive data change notifications for the same neighbor

If LLDP trap notification is enabled on a port, a rapid succession of changes in LLDP information received in advertisements from one or more neighbors can generate a high number of traps. To reduce this effect, you can globally change the interval between successive notifications of neighbor data change.

Basic LLDP per-port advertisement content

In the default LLDP configuration, outbound advertisements from each port on the switch include both mandatory and optional data.

Mandatory Data

An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. LLDP collects the mandatory data, and, except for the Remote Management Address, you cannot use LLDP commands to configure the actual data.

- Chassis Type (TLV subelement)
- Chassis ID (TLV)

- Port Type (TLV subelement)
- Port ID (TLV)
- Remote Management Address (TLV; actual IP address is a subelement that can be a default address or a configured address)

Optional Data

You can configure an individual port or group of ports to exclude one or more of the following data types from outbound LLDP advertisements.

- Port description (TLV)
- System name (TLV)
- System description (TLV)
- System capabilities (TLV)
  - System capabilities Supported (TLV subelement)
  - System capabilities Enabled (TLV subelement)
- Port speed and duplex (TLV subelement)

Optional data types, when enabled, are populated with data internal to the switch; that is, you cannot use LLDP commands to configure their actual content.

Support for port speed and duplex advertisements

This feature is optional for LLDP operation, but is *required* for LLDP-MED operation.

Port speed and duplex advertisements are supported on the switches to inform an LLDP endpoint and the switch port of each other's port speed and duplex configuration and capabilities. Configuration mismatches between a switch port and an LLDP endpoint can result in excessive collisions and voice quality degradation. LLDP enables discovery of such mismatches by supporting SNMP access to the switch MIB for comparing the current switch port and endpoint settings. (Changing a current device configuration to eliminate a mismatch requires intervention by the system operator.)

An SNMP network management application can be used to compare the port speed and duplex data configured in the switch and advertised by the LLDP endpoint. You can also use the CLI to display this information. For more information on using the CLI to display port speed and duplex information, see“Viewing the current port speed and duplex configuration on a switch port” (page 209).

Port VLAN ID TLV support on LLDP

The `port-vlan-id` option enables advertisement of the port VLAN ID TLV as part of the regularly advertised TLVs. This allows discovery of a mismatch in the configured native VLAN ID between LLDP peers. The information is visible using `show` commands and is logged to the Syslog server.

SNMP support

The LLDP-EXT-DOT1-MIB has the corresponding MIB variables for the Port VLAN ID TLV. The TLV advertisement can be enabled or disabled using the MIB object `lldpXdot1ConfigPortVlanTxEnable` in the `lldpXdot1ConfigPortVlanTable`.

The port VLAN ID TLV local information can be obtained from the MIB object `lldpXdot1LocPortVlanId` in the local information table `lldpXdot1LocTable`.

The port VLAN ID TLV information about all the connected peer devices can be obtained from the MIB object `lldpXdot1RemPortVlanId` in the remote information table `lldpXdot1RemTable`.

LLDP-MED (media-endpoint-discovery)

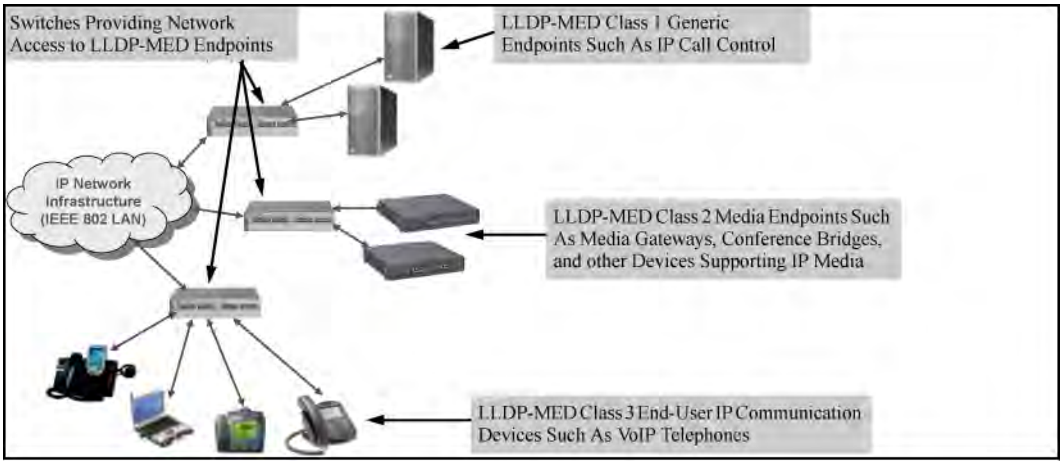
LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP (IEEE 802.1AB) industry standard to support advanced features on the network edge for Voice Over IP (VoIP) endpoint devices with specialized capabilities and LLDP-MED standards-based functionality. LLDP-MED in the switches uses the standard LLDP commands described earlier in this section, with some extensions, and also introduces new commands unique to LLDP-MED operation. The `show` commands described elsewhere in this section are applicable to both LLDP and LLDP-MED operation. LLDP-MED benefits include:

- Plug-and-play provisioning for MED-capable, VoIP endpoint devices
- Simplified, vendor-independent management enabling different IP telephony systems to interoperate on one network
- Automatic deployment of convergence network policies (voice VLANs, Layer 2/CoS priority, and Layer 3/QoS priority)
- Configurable endpoint location data to support the Emergency Call Service (ECS) (such as Enhanced 911 service, 999, 112)
- Detailed VoIP endpoint data inventory readable via SNMP from the switch
- Power over Ethernet (PoE) status and troubleshooting support via SNMP
- support for IP telephony network troubleshooting of call quality issues via SNMP

This section describes how to configure and use LLDP-MED features in the switches to support VoIP network edge devices (media endpoint devices) such as:

- IP phones
- Voice/media gateways
- Media servers
- IP communications controllers
- Other VoIP devices or servers

Figure 107 Example of LLDP-MED network elements


Switches Providing Network Access to LLDP-MED Endpoints
LLDP-MED Class 1 Generic Endpoints Such As IP Call Control
IP Network Infrastructure (IEEE 802 LAN)
LLDP-MED Class 2 Media Endpoints Such As Media Gateways, Conference Bridges, and other Devices Supporting IP Media
LLDP-MED Class 3 End-User IP Communication Devices Such As VoIP Telephones

LLDP-MED endpoint support

LLDP-MED interoperates with directly connected IP telephony (endpoint) clients having these features and services:

- Autonegotiate speed and duplex configuration with the switch
- Use the following network policy elements configured on the client port
- Voice VLAN ID

- 802.1p (Layer 2) QoS
- Diffserv codepoint (DSCP) (Layer 3) QoS
- Discover and advertise device location data learned from the switch
- Support ECS (such as E911, 999, and 112)
- Advertise device information for the device data inventory collected by the switch, including:

• Hardware revision	• Serial number	• Asset ID
• Firmware revision	• Manufacturer name	
• Software revision	• Model name	

- Provide information on network connectivity capabilities (for example, a multi-port VoIP phone with Layer 2 switch capability)
- Support the fast-start capability

NOTE: LLDP-MED is intended for use with VoIP endpoints and is not designed to support links between network infrastructure devices, such as switch-to-switch or switch-to-router links.

LLDP-MED endpoint device classes

LLDP-MED endpoint devices are, by definition, located at the network edge and communicate using the LLDP-MED framework. Any LLDP-MED endpoint device belongs to one of the following three classes:

- Class 1 (generic endpoint devices): These devices offer the basic LLDP discovery services, network policy advertisement (VLAN ID, Layer 2/802.1p priority, and Layer 3/DSCP priority), and PoE management. This class includes such devices as IP call controllers and communication-related servers.
- Class 2 (media endpoint devices): These devices offer all Class 1 features plus media-streaming capability, and include such devices as voice/media gateways, conference bridges, and media servers.
- Class 3 (communication devices): These devices are typically IP phones or end-user devices that otherwise support IP media and offer all Class 1 and Class 2 features, plus location identification and emergency 911 capability, Layer 2 switch support, and device information management.

LLDP-MED operational support

The switches offer two configurable TLVs supporting MED-specific capabilities:

- medTlvEnable (for per-port enabling or disabling of LLDP-MED operation)
- medPortLocation (for configuring per-port location or emergency call data)

NOTE: LLDP-MED operation also requires the port speed and duplex TLV (dot3TlvEnable; page 14-41), which is enabled in the default configuration.

Topology change notifications provide one method for monitoring system activity. However, because SNMP normally employs UDP, which does not guarantee datagram delivery, topology change notification should not be relied upon as the sole method for monitoring critical endpoint device connectivity.

Advertising device capability, network policy, PoE status and location data

The medTlvEnable option on the switch is enabled in the default configuration and supports the following LLDP-MED TLVs:

- LLDP-MED capabilities: This TLV enables the switch to determine:
  - Whether a connected endpoint device supports LLDP-MED
  - Which specific LLDP-MED TLVs the endpoint supports
  - The device class (1, 2, or 3) for the connected endpoint

  This TLV also enables an LLDP-MED endpoint to discover what LLDP-MED TLVs the switch port currently supports.
- Network policy operating on the port to which the endpoint is connected (VLAN, Layer 2 QoS, Layer 3 QoS)
- PoE (MED Power-over-Ethernet)
- Physical location data (see Configuring location data for LLDP-MED devices (page 205))

NOTE: LLDP-MED operation requires the macphy_config TLV subelement (enabled by default) that is optional for IEEE 802.1AB LLDP operation. For more information, see the `dot3TlvEnable macphy_config` command ("Configuring support for port speed and duplex advertisements (CLI)" (page 201)).

Network policy advertisements

Network policy advertisements are intended for real-time voice and video applications, and include these TLV subelements:

- Layer 2 (802.1p) QoS
- Layer 3 DSCP (diffserv code point) QoS
- Voice VLAN ID (VID)

VLAN operating rules

These rules affect advertisements of VLANs in network policy TLVs:

- The VLAN ID TLV subelement applies only to a VLAN configured for voice operation (`vlan` *`vid`* `voice`).
- If there are multiple voice VLANs configured on a port, LLDP-MED advertises the voice VLAN having the lowest VID.
- The voice VLAN port membership configured on the switch can be tagged or untagged. However, if the LLDP-MED endpoint expects a tagged membership when the switch port is configured for untagged, or the reverse, a configuration mismatch results. (Typically, the endpoint expects the switch port to have a tagged voice VLAN membership.)
- If a given port does not belong to a voice VLAN, the switch does not advertise the VLAN ID TLV through this port.

Policy elements

These policy elements may be statically configured on the switch or dynamically imposed during an authenticated session on the switch using a RADIUS server and 802.1X or MAC authentication. (Web authentication does not apply to VoIP telephones and other telecommunications devices that are not capable of accessing the switch through a Web browser.) The QoS and voice VLAN policy elements can be statically configured with the following CLI commands:

```
vlan vid voice
vlan  vid   tagged | untagged
port-list
int  port-list  qos priority  0 - 7
vlan  vid  qos dscp  codepoint
```

NOTE: A codepoint must have an 802.1p priority before you can configure it for use in prioritizing packets by VLAN-ID. If a codepoint you want to use shows `No Override` in the `Priority` column of the DSCP policy table (display with `show qos-dscp map`, then use `qos-dscp map` *`codepoint`* `priority  0 - 7` to configure a priority before proceeding. For more information on this topic, see the chapter "Quality of Service (QoS): Managing Bandwidth More Effectively" in the *Advanced Traffic Management Guide* for your switch.

PoE advertisements

These advertisements inform an LLDP-MED endpoint of the power (PoE) configuration on switch ports. Similar advertisements from an LLDP-MED endpoint inform the switch of the endpoint's power needs and provide information that can be used to identify power priority mismatches.

PoE TLVs include the following power data:

- **Power type**: indicates whether the device is a power-sourcing entity (PSE) or a PD. Ports on the J8702A PoE zl module are PSE devices. A MED-capable VoIP telephone is a PD.
- **Power source**: indicates the source of power in use by the device. Power sources for PDs include PSE, local (internal), and PSE/local. The switches advertise Unknown.
- **Power priority**: indicates the power priority configured on the switch (PSE) port or the power priority configured on the MED-capable endpoint.
- **Power value**: indicates the total power in watts that a switch port (PSE) can deliver at a particular time, or the total power in watts that the MED endpoint (PD) requires to operate.

Location data for LLDP-MED devices

You can configure a switch port to advertise location data for the switch itself, the physical wall-jack location of the endpoint (recommended), or the location of a DHCP server supporting the switch, endpoint, or both. You also have the option of configuring these different address types:

- **Civic address**: physical address data such as city, street number, and building information
- **ELIN (Emergency Location Identification Number)**: an emergency number typically assigned to MLTS (Multiline Telephone System) Operators in North America
- **Coordinate-based location**: attitude, longitude, and altitude information (Requires configuration via an SNMP application.)

About configuring coordinate-based locations

Latitude, longitude, and altitude data can be configured per switch port using an SNMP management application. For more information, see the documentation provided with the application. A further source of information on this topic is *RFC 3825-Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information*.

NOTE: Endpoint use of data from a medPortLocation TLV sent by the switch is device-dependent. See the documentation provided with the endpoint device.

Table 26 Some location codes used in CA-TYPE fields[1]

Location element	Code	Location element	Code
national subdivision	1	street number	19
regional subdivision	2	additional location data	22
city or township	3	unit or apartment	26
city subdivision	4	floor	27
street	6	room number	28
street suffix	18		

[1] The code assignments in this table are examples from a work-in-progress (the internet draft titled "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information draft-ietf-geopriv-dhcp-civil-06" dated May 30, 2005.) For the actual codes to use, contact the PSAP or other authority responsible for specifying the civic addressing data standard for your network.

Example

Suppose a system operator wants to configure the following information as the civic address for a telephone connected to her company's network through port A2 of a switch at the following location:

Description	CA-type	CA-VALUE
national subdivision	1	CA
city	3	Widgitville
street	6	Main
street number	19	1433
unit	26	Suite 4-N
floor	27	4
room number	28	N4-3

Example 50 (page 237) shows the commands for configuring and displaying the above data.

Example 50 Example of a civic address configuration

```
HP Switch(config)# lldp config 2 medportlocation civic-addr US 2 1 CA 3
Widgitville 6 Main 19 1433 26 Suite_4–N 27 4 28 N4–3

HP Switch(config)# show lldp config 2
 LLDP Port Configuration Detail
  Port : A2
  AdminStatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False
  Country Name           : US
  What                   : 2
  Ca-Type                : 1
  Ca-Length              : 2
  Ca-Value               : CA
  Ca-Type                : 3
  Ca-Length              : 11
  Ca-Value               : Widgitville
  Ca-Type                : 6
  Ca-Length              : 4
  Ca-Value               : Main
  Ca-Type                : 19
  Ca-Length              : 4
  Ca-Value               : 1433
  Ca-Type                : 26
  Ca-Length              : 9
  Ca-Value               : Suite_4-N
  Ca-Type                : 27
  Ca-Length              : 1
  Ca-Value               : 4
  Ca-Type                : 28
  Ca-Length              : 4
  Ca-Value               : N4-3
```

About displaying the current port speed and duplex configuration on a switch port

You can compare port speed and duplex information for a switch port and a connected LLDP-MED endpoint for configuration mismatches by using an SNMP application. You can also use the switch CLI to display this information, if necessary. The `show interfaces brief` *`port-list`* (Example 17 (page 53)) and `show lldp info remote-device [`*`port-list`*`]` (Figure 34 (page 89)) commands provide methods for displaying speed and duplex information for switch ports. For information on displaying the currently configured port speed and duplex on an LLDP-MED endpoint, see“Viewing the current port speed and duplex configuration on a switch port” (page 209).

Displaying LLDP statistics

LLDP statistics are available on both a global and a per-port levels. Rebooting the switch resets the LLDP statistics counters to zero. Disabling the transmit and/or receive capability on a port "freezes" the related port counters at their current values.

LLDP Operating Notes

Neighbor maximum

The neighbors table in the switch supports as many neighbors as there are ports on the switch. The switch can support multiple neighbors connected through a hub on a given port, but if the switch neighbor maximum is reached, advertisements from additional neighbors on the same or other ports will not be stored in the neighbors table unless some existing neighbors time-out or are removed.

LLDP packet forwarding

An 802.1D-compliant switch does not forward LLDP packets, regardless of whether LLDP is globally enabled or disabled on the switch.

One IP address advertisement per port

LLDP advertises only one IP address per port, even if multiple IP addresses are configured by `lldp config` *`port-list`* `ipAddrEnable` (see syntax (page 200)) on a given port.

802.1Q VLAN Information

LLDP packets do not include 802.1Q header information and are always handled as untagged packets.

Effect of 802.1X Operation

If 802.1X port security is enabled on a port, and a connected device is not authorized, LLDP packets are not transmitted or received on that port. Any neighbor data stored in the neighbor MIB for that port prior to the unauthorized device connection remains in the MIB until it ages out. If an unauthorized device later becomes authorized, LLDP transmit and receive operation resumes.

Neighbor data can remain in the neighbor database after the neighbor is disconnected

After disconnecting a neighbor LLDP device from the switch, the neighbor can continue to appear in the switch's neighbor database for an extended period if the neighbor's `holdtime-multiplier` is high; especially if the `refresh-interval` is large. See "Changing the time-to-live for transmitted advertisements (CLI)" (page 197).

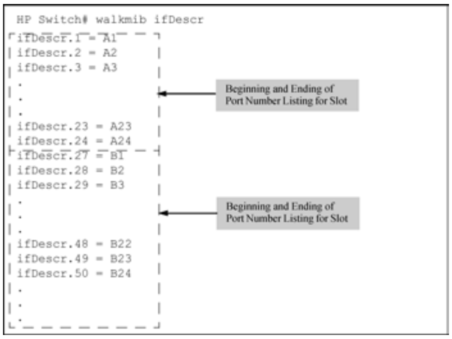
Mandatory TLVs

All mandatory TLVs required for LLDP operation are also mandatory for LLDP-MED operation.

About determining the switch port number included in topology change notification traps

Enabling topology change notification on a switch port and then connecting or disconnecting an LLDP-MED endpoint on that port causes the switch to send an SNMP trap to notify the designated management stations. The port number included in the trap corresponds to the internal number the switch maintains for the designated port, and not the port's external (slot/number) identity. To match the port's external slot/number to the internal port number appearing in an SNMP trap, use the `walkmib ifDescr` command, as shown in Figure 108 (page 238).

Figure 108 Matching internal port numbers to external slot/port numbers



```
HP Switch# walkmib ifDescr
ifDescr.1 = A1
ifDescr.2 = A2
ifDescr.3 = A3
.
.
.
ifDescr.23 = A23
ifDescr.24 = A24
ifDescr.27 = B1
ifDescr.28 = B2
ifDescr.29 = B3
.
.
.
ifDescr.48 = B22
ifDescr.49 = B23
ifDescr.50 = B24
.
.
.
```

Beginning and Ending of Port Number Listing for Slot
Beginning and Ending of Port Number Listing for Slot

LLDP and CDP data management

This section describes points to note regarding LLDP and CDP (Cisco Discovery Protocol) data received by the switch from other devices. LLDP operation includes both transmitting LLDP packets to neighbor devices and reading LLDP packets received from neighbor devices. CDP operation is limited to reading incoming CDP packets from neighbor devices. (HP switches do not generate CDP packets.)

Incoming CDP and LLDP packets tagged for VLAN 1 are processed even if VLAN 1 does not contain any ports. VLAN 1 must be present, but it is typically present as the default VLAN for the switch.

NOTE: The switch may pick up CDP and LLDP multicast packets from VLAN 1 even when CDP- and /or LLDP-enabled ports are not members of VLAN 1.

LLDP and CDP neighbor data

With both LLDP and (read-only) CDP enabled on a switch port, the port can read both LLDP and CDP advertisements, and stores the data from both types of advertisements in its neighbor database. (The switch *stores* only CDP data that has a corresponding field in the LLDP neighbor database.) The neighbor database itself can be read by either LLDP or CDP methods or by using the `show lldp` commands. Take note of the following rules and conditions:

- If the switch receives both LLDP and CDP advertisements on the same port from the same neighbor, the switch stores this information as two separate entries if the advertisements have different chassis ID and port ID information.
- If the chassis and port ID information are the same, the switch stores this information as a single entry. That is, LLDP data overwrites the corresponding CDP data in the neighbor database if the chassis and port ID information in the LLDP and CDP advertisements received from the same device is the same.
- Data read from a CDP packet does not support some LLDP fields, such as "System Descr," "SystemCapSupported," and "ChassisType." For such fields, LLDP assigns relevant default values. Also:
    - The LLDP "System Descr" field maps to CDP's "Version" and "Platform" fields.
    - The switch assigns "ChassisType" and "PortType" fields as "local" for both the LLDP and the CDP advertisements it receives.
    - Both LLDP and CDP support the "System Capability" TLV. However, LLDP differentiates between what a device is capable of supporting and what it is actually supporting, and separates the two types of information into subelements of the System Capability TLV. CDP has only a single field for this data. Thus, when CDP System Capability data is mapped to LLDP, the same value appears in both LLDP System Capability fields.
    - System Name and Port Descr are not communicated by CDP, and thus are not included in the switch's Neighbors database.

NOTE: Because HP switches do not generate CDP packets, they are not represented in the CDP data collected by any neighbor devices running CDP.

A switch with CDP disabled forwards the CDP packets it receives from other devices, but does not store the CDP information from these packets in its own MIB.

LLDP data transmission/collection and CDP data collection are both enabled in the switch's default configuration. In this state, an SNMP network management application designed to discover devices running either CDP or LLDP can retrieve neighbor information from the switch regardless of whether LLDP or CDP is used to collect the device-specific information.

Protocol state	Packet generation	Inbound data management	Inbound packet forwarding
CDP Enabled[1]	N/A	Store inbound CDP data.	No forwarding of inbound CDP packets.
CDP Disabled	N/A	No storage of CDP data from neighbor devices.	Floods inbound CDP packets from connected devices to outbound ports.

Protocol state	Packet generation	Inbound data management	Inbound packet forwarding
LLDP Enabled[1]	Generates and transmits LLDP packets out all ports on the switch.	Store inbound LLDP data.	No forwarding of inbound LLDP packets.
LLDP Disabled	No packet generation.	No storage of LLDP data from neighbor devices.	No forwarding of inbound LLDP packets.

[1] Both CDP data collection and LLDP transmit/receive are enabled in the default configuration. If a switch receives CDP packets and LLDP packets from the same neighbor device on the same port, it stores and displays the two types of information separately if the chassis and port ID information in the two types of advertisements is different. In this case, if you want to use only one type of data from a neighbor sending both types, disable the unwanted protocol on either the neighbor device or on the switch. However, if the chassis and port ID information in the two types of advertisements is the same, the LLDP information overwrites the CDP data for the same neighbor device on the same port.

CDP operation and commands

By default the switches have CDP enabled on each port. This is a read-only capability, meaning that the switch can receive and store information about adjacent CDP devices but does not generate CDP packets.

When a CDP-enabled switch receives a CDP packet from another CDP device, it enters that device's data in the CDP Neighbors table, along with the port number where the data was received—and does not forward the packet. The switch also periodically purges the table of any entries that have expired. (The hold time for any data entry in the switch's CDP Neighbors table is configured in the device transmitting the CDP packet and cannot be controlled in the switch receiving the packet.) A switch reviews the list of CDP neighbor entries every three seconds and purges any expired entries.

NOTE: For details on how to use an SNMP utility to retrieve information from the switch's CDP Neighbors table maintained in the switch's MIB, see the documentation provided with the particular SNMP utility.

8 Chassis Redundancy (8200zl Switches)

Command Summary

Table 27 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
show redundancy	Displays the status of the management and fabric modules.	-	(page 241)	-
[no] redundancy management-module [nonstop-switching]	Allows enabling or disabling of redundant management.	Warmstandby redundancy mode	(page 242)	-
redundancy rapid-switchover 0-2147483647	Allows configuration of a timer (in seconds) for Layer 3 forwarding of packets when nonstop switching is configured for redundancy.	45 seconds	(page 247)	-
redundancy switchover	Causes a switchover to the standby module.	-	(page 248)	-
redundancy active-management management-module1 | management-module2 | standby	The specified module becomes the active management module at the next system boot.	-	(page 248)	-
show modules [details]	Displays information about the installed modules.	-	(page 251)	-
boot set-default flash primary | secondary	Sets the flash image to boot from on the next boot.	-	(page 256)	-
reload cr	Boots (warm reboot) the active management module.	-	(page 257)	-
show logging [-a, -b, -r, -s, -t, -m, -p, -w, -i, -d, *option-str*]	Displays messages about the activities and status of the management modules.	-	(page 258)	-
copy crash-log [*slot-id* | mm] tftp *ip-address filename*	Copies the crash logs of both the active and standby management modules to a user-specified file.	-	(page 259)	-
copy crash-data [*slot-id* | mm] tftp *ip-address filename*	Copies the crash data of both the active and standby management modules to a user-specified file.	-	(page 259)	-
redundancy fabric-module [1 | 2] [enable | disable]	Enables or disables redundant fabric modules.	Enabled	(page 260)	-

For an overview of Chassis Redundancy, see "Overview of chassis redundancy (8200zl switches)" (page 261).

For information about how to use redundant management, see "About using redundant management" (page 262).

Viewing management module redundancy status (CLI)

You can display the status of both the management and fabric redundant modules using this command:

Syntax:

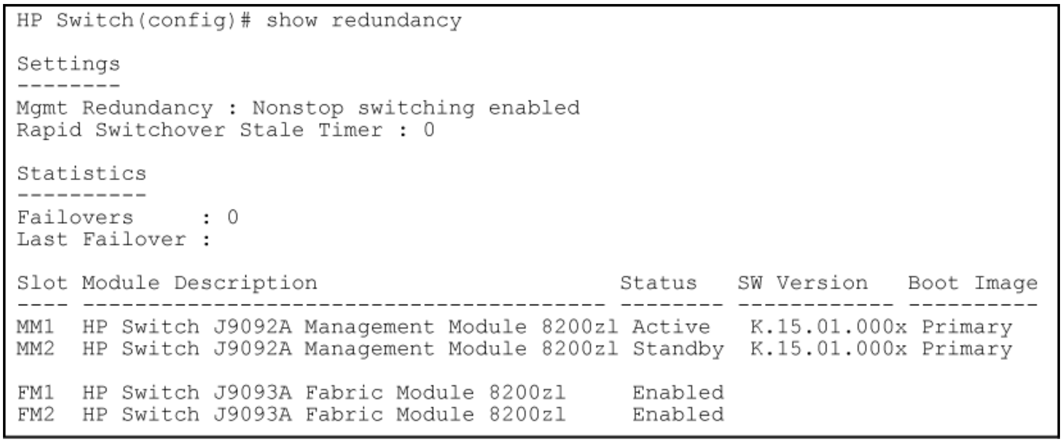
`show redundancy`

Displays the status of the management and fabric modules.

Example

The output for the `show redundancy` command is seen in Figure 109 (page 242).

Figure 109 `show redundancy` command for management and fabric modules



```
HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop switching enabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                        Status   SW Version   Boot Image
---- ---------------------------------------- -------- ------------ ----------
MM1  HP Switch J9092A Management Module 8200zl Active   K.15.01.000x Primary
MM2  HP Switch J9092A Management Module 8200zl Standby  K.15.01.000x Primary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Enabled
```

Enabling or disabling redundant management (CLI)

For more information, see "How the management modules interact" (page 261).

There are two modes for management module redundancy—warm standby mode (the default) and Nonstop switching mode. In warm-standby mode, the active management module does not sync continuously with the standby management module. The standby management module boots to a certain point, syncs basic files, and only finishes booting if the active management module fails or you choose to change which module is the active management module. The transition is not seamless or immediate.

In Nonstop switching mode, the standby management module is synced continuously with the active management module so that all features and config files are the same on both management modules. The standby management module is ready to become the active management module. The transition is quick and seamless; switching continues without interruption.

Syntax:

[no] `redundancy management-module` [`nonstop-switching`]

Allows enabling or disabling of redundant management. The current active module continues to be the active module on boot unless you use the `redundancy active-management` command to enable redundant behavior.

(Default: Warm-standby redundancy mode)

The `nonstop-switching` parameter sets the redundancy mode to Nonstop switching.

You are prompted with "All configuration files and software images on the off-line management module will be overwritten with the data from the current active management module. During initial syncing from active to standby management module configuration changes are disallowed. Do you want to continue [y/n]?"

When the `nonstop-switching` option is *not* selected, the switch enters warm-standby redundancy mode.

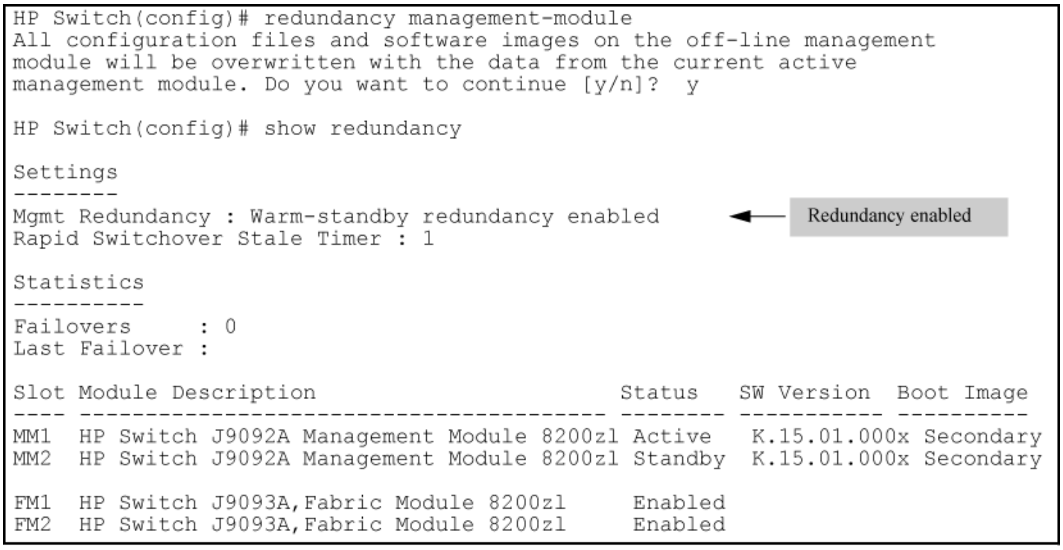
You are prompted with "All configuration files and software images on the off-line management module will be overwritten with the data from the current active management module. Do you want to continue [y/n]?"

The `no` version of the command disables redundant management. You are prompted with this message: "The other management module may reboot and it will no longer be used for system redundancy, except in the case of a hardware failure of the active management module. Do you want to continue [y/n]?".

Example

The `redundancy management-module` command in Figure 110 (page 243) shows **warm-standby redundant management** being **enabled**. The `show redundancy` command displays "**Mgmt Redundancy**" as ***warm-standby redundancy enabled***. Management Module 1 (MM1) is the active management module and Management Module 2 (MM2) is the standby management module.

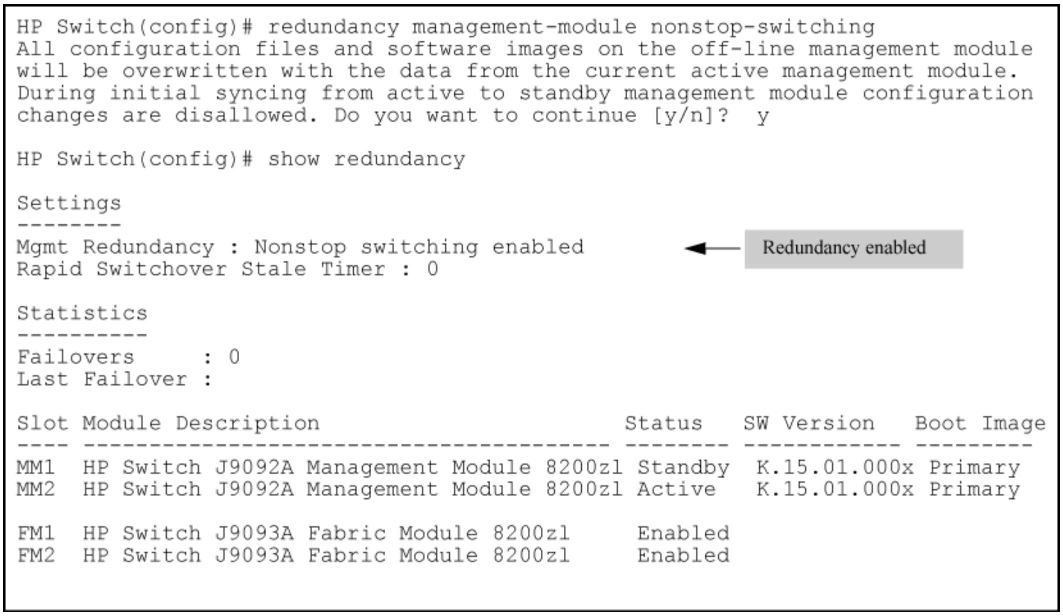
Figure 110 Enabling warm-standby redundancy



```
HP Switch(config)# redundancy management-module
All configuration files and software images on the off-line management
module will be overwritten with the data from the current active
management module. Do you want to continue [y/n]?  y

HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Warm-standby redundancy enabled
Rapid Switchover Stale Timer : 1

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                        Status   SW Version  Boot Image
---- ---------------------------------------- -------- ----------- ----------
MM1  HP Switch J9092A Management Module 8200zl Active   K.15.01.000x Secondary
MM2  HP Switch J9092A Management Module 8200zl Standby  K.15.01.000x Secondary

FM1  HP Switch J9093A,Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A,Fabric Module 8200zl     Enabled
```

The `redundancy management-module` command in Figure Figure 111 (page 244) shows Non-stop switching redundant management being **enabled**. The `show redundancy` command displays "**Mgmt Redundancy**" as ***Nonstop switching enabled***. Management Module 1 (MM1) is the standby management module and Management Module 2 (MM2) is the active management module.

Figure 111 Enabling nonstop-switching redundancy



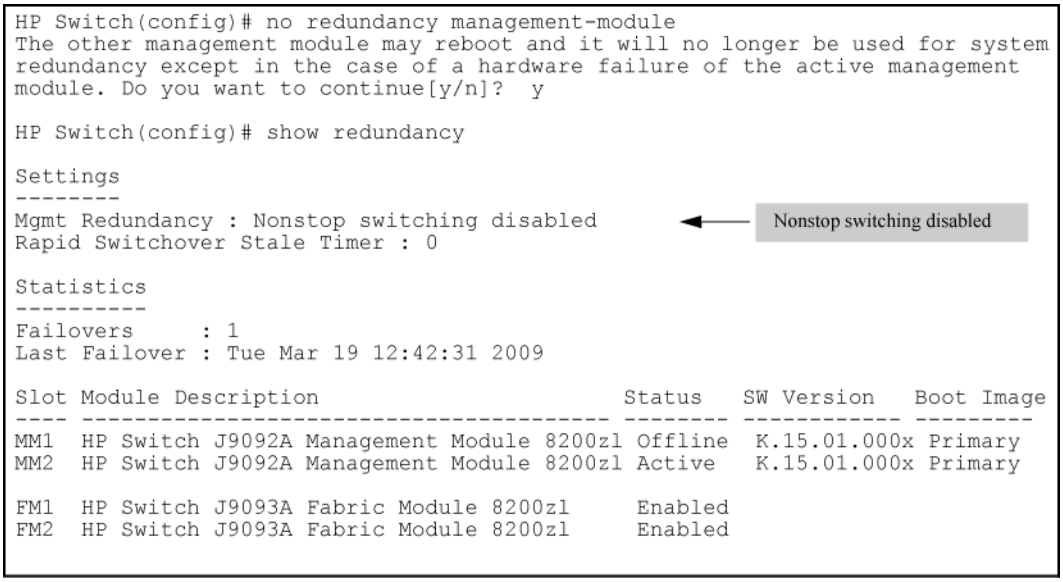
```
HP Switch(config)# redundancy management-module nonstop-switching
All configuration files and software images on the off-line management module
will be overwritten with the data from the current active management module.
During initial syncing from active to standby management module configuration
changes are disallowed. Do you want to continue [y/n]?  y

HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop switching enabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                           Status   SW Version   Boot Image
---- ---------------------------------------- -------- ------------ ---------
MM1  HP Switch J9092A Management Module 8200zl Standby  K.15.01.000x Primary
MM2  HP Switch J9092A Management Module 8200zl Active   K.15.01.000x Primary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Enabled
```

The no version of the `redundancy management-module` command is used to disable management module redundancy on the switch, as seen in Figure Figure 112 (page 244). The `show redundancy` command displays "**Mgmt Redundancy**" as ***Nonstop switching disabled***. The standby management module in slot MM1 is now offline. The management module in slot MM2 remains the active management module.

NOTE: HP recommends that you leave management module redundancy enabled. If the active management module has a hardware failure, the standby module may take over and may have an old configuration since file synchronization has not occurred when management module redundancy was disabled.

The `no redundancy management-module` command allows you to shut down a management module that is not functioning correctly without physically removing the module. If you want to remove the module, first perform the shutdown procedure as explained in "Hotswapping out the active management module" (page 250) and then remove the module.

Figure 112 Disabling redundancy



```
HP Switch(config)# no redundancy management-module
The other management module may reboot and it will no longer be used for system
redundancy except in the case of a hardware failure of the active management
module. Do you want to continue[y/n]?  y

HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop switching disabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 1
Last Failover : Tue Mar 19 12:42:31 2009

Slot Module Description                           Status   SW Version   Boot Image
---- ---------------------------------------- -------- ------------ ---------
MM1  HP Switch J9092A Management Module 8200zl Offline  K.15.01.000x Primary
MM2  HP Switch J9092A Management Module 8200zl Active   K.15.01.000x Primary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Enabled
```

The `redundancy management-module` command shows Nonstop switching redundant management being enabled. The `show redundancy` command displays "Mgmt Redundancy" as Nonstop switching enabled. Management Module 1 (MM1) is the standby management module and Management Module 2 (MM2) is the active management module.

Enabling non-stop switching redundancy

```
HP Switch(config)# redundancy management-module nonstop-switching
All configuration files and software images on the off-line management module
will be overwritten with the data from the current active management module.
During initial syncing from active to standby management module configuration
changes are disallowed. Do you want to continue [y/n]? y
HP Switch(config)# show redundancy
Settings
--------
Mgmt Redundancy : Nonstop switching enabled
Rapid Switchover Stale Timer : 0
Statistics
----------
Failovers : 0
Last Failover :
Slot Module    Description                 Status   SW Version    Boot Image
---- ---------------------------------------   ----------    ------------
MM1  HP J9092A Management Module 8200zl  Standby  K.15.01.000x  Primary
MM2  HP J9092A Management Module 8200zl  Active   K.15.01.000x  Primary
FM1  HP J9093A Fabric Module 8200zl      Enabled
FM2  HP J9093A Fabric Module 8200zl      Enabled
```

The no version of the redundancy management-module command is used to disable management module redundancy on the switch, as seen in Figure 7-4. The show redundancy command displays "Mgmt Redundancy" as Nonstop switching disabled. The standby management module in slot MM1 is now offline. The management module in slot MM2 remains the active management module.

NOTE: HP recommends that you leave management module redundancy enabled. If the active management module has a hardware failure, the standby module may take over and may have an old configuration since file synchronization has not occurred when management module redundancy was disabled.

The `no redundancy management-module` command allows you to shut down a management module that is not functioning correctly without physically removing the module. If you want to remove the module, first perform the shutdown procedure as explained in "Hotswapping Out the Active Management Module" on page 7-25, and then remove the module.

Disabling redundancy

```
HP Switch(config)# no redundancy management-module
The other management module may reboot and it will no longer be used for system
redundancy except in the case of a hardware failure of the active management
module. Do you want to continue[y/n]? y
HP Switch(config)# show redundancy
Settings
--------
Mgmt Redundancy : Nonstop switching disabled
Rapid Switchover Stale Timer : 0
Statistics
----------
Failovers : 1
Last Failover : Tue Mar 19 12:42:31 2009
Slot   Module     Description              Status   SW Version   Boot Image
----   ---------  ------------------------ -------  -----------   ------------
MM1    HP J9092A  Management Module 8200zl Offline  K.15.01.000x  Primary
MM2    HP J9092A  Management Module 8200zl Active   K.15.01.000x  Primary
FM1    HP J9093A  Fabric Module 8200zl     Enabled
FM2    HP J9093A  Fabric Module 8200zl     Enabled
```

Transitioning from no `redundancy` to nonstop switching

While the switch is transitioning from no redundancy mode to Nonstop switching mode, no configuration changes are allowed. The management modules are syncing information during the transition period.

Setting the Rapid Switchover Stale Timer

Use the Rapid Switchover Stale Timer to set the amount of time that you want route and neighbor table entries to be re-added to the Forwarding Information Base on the active management module after a failover has occurred.

Layer 3 applications and protocols rely on existing routing information in the FIB. They restart and operate as if the switch performed a quick reset.

When a failover occurs, the interface modules and the fabric modules continue forwarding Layer 3 traffic based on the information in the FIB. The transitioning standby management module marks all routes in the FIB as "stale". The routing protocols restart, reestablish their neighbors and reconverge. As the routes are added in again, the route's stale designation is removed. After the Rapid Switchover Stale Timer expires, the remaining stale route entries are removed. Multicast flows are also removed; the multicast application re-adds the flows after failover completes.

Syntax

```
redundancy rapid-switchover <0-2147483647>
```

Allows configuration of a timer (in seconds) for Layer 3 forwarding of packets when Nonstop switching is configured for redundancy. After failover, the route and neighbor entries in the Forwarding Information Base (FIB) on the active management module are marked as stale. As new routes are added, the stale flag is reset. This continues for the number of seconds indicated by the timer, after which all remaining stale entries (entries not re-added) are removed.

A setting of zero indicates that no Layer 3 Nonstop switching behavior is wanted.

When the switch fails over, the FIB entries and corresponding hardware entries are removed. Default: 90 seconds

To display information about stale FIB routes, enter the show tech route stale command. The VLAN ID and IP route are shown, as well as other information used only for technical support.

Directing the standby module to become active

To make the standby management module become the active management module, use the `redundancy switchover` command. The switch will switchover after all files have finished synchronizing.

In Nonstop switching mode:

- The switchover occurs quickly and seamlessly. No reboot is needed.
- There is no interruption in switching operations.

In warm-standby mode:

- The switchover may take a couple of minutes if there have been recent configuration file changes or if you have downloaded a new operating system.
- The standby module finishes booting and becomes the active module.

The formerly active module becomes the standby module if it passes selftest.

Syntax

```
redundancy switchover
```

Causes a switchover to the standby module.

For Nonstop switching, the warning displays:`A nonstop switching failover will occur; L2 operations will not be interrupted. This management module will now reboot and will become the standby module! You will need to use the other management module’s console interface. Do you want to continue [y/n]?`

In warm-standby mode the warning displays:`A warm failover will occur; all networking operations will be interrupted. This management module will now reboot and will become the standby module! You will need to use the other management module’s console interface. Do you want to continue [y/n]?`

If management module redundancy has been disabled, or there is no standby module, or the standby module is not in standby mode, this message displays:`The other management module does not exist or is not in standby mode` An example of the `redundancy switchover` command when the switch is in Nonstop switching mode is shown in the example below.

`Redundancy switchover` command when in nonstop switching mode

```
HP Switch(config)# redundancy switchover
A nonstop switching failover will occur; L2 operations will not be interrupted.
This management module will now reboot and will become the standby
module! You will need to use the other management module's console interface.
Do you want to continue [y/n]? y
This management module will now boot from the primary image and will
become the standby module! You will need to used the other management module’s
console interface. Do you want to continue [y/n]? y
ROM information:
Build directory: /sw/rom/build/bmrom(t2g)
Build date: Oct 15 2009
Build time: 08:24:27
Build version: K.15.01
Build number: 13040
Select profile (primary):
Booting Primary Software Image...
...
Standby Console>
```

Setting the rapid switchover stale timer (CLI)

For more information about transitioning from no redundancy to nonstop switching and setting the rapid switchover stale timer, see“Transition from no redundancy to nonstop switching” (page 262)and “About setting the rapid switchover stale timer” (page 262).

Syntax:

`redundancy rapid-switchover 0-2147483647`

Allows configuration of a timer (in seconds) for Layer 3 forwarding of packets when nonstop switching is configured for redundancy. After failover, the route and neighbor entries in the forwarding information base (FIB) on the active management module are marked as stale. As new routes are added, the stale flag is reset. This continues for the number of seconds indicated by the timer, after which all remaining stale entries (entries not re-added) are removed.

A setting of zero indicates that no Layer 3 Nonstop switching behavior is wanted. When the switch fails over, the FIB entries and corresponding hardware entries are removed.

(Default: 45 seconds)

To display information about stale FIB routes, enter the `show tech route stale` command. The VLAN ID and IP route are shown, as well as other information used only for technical support.

Directing the standby module to become active (CLI)

For more information, see "About directing the standby module to become active" (page 262).

Syntax:

```
redundancy switchover
```

Causes a switchover to the standby module.

For nonstop switching, the warning displays: "A nonstop switching failover will occur; L2 operations will not be interrupted. This management module will now reboot and will become the standby module! You will need to use the other management module's console interface. Do you want to continue [y/n]?"

In warm-standby mode the warning displays: "A warm failover will occur; all networking operations will be interrupted. This management module will now reboot and will become the standby module! You will need to use the other management module's console interface. Do you want to continue [y/n]?"

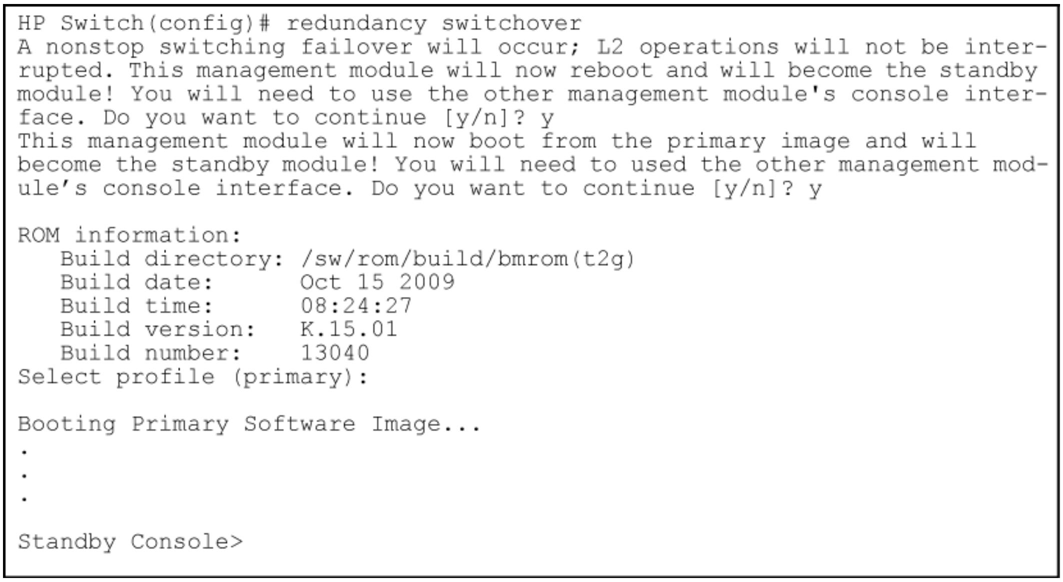
If management module redundancy has been disabled, or if there is no standby module, or if the standby module is not in standby mode, this message displays:

```
The other management module does not exist or is not in standby mode
```

Example

Figure 113 (page 248) shows an example of the `redundancy switchover` command when the switch is in **nonstop switching** mode.

Figure 113 The `redundancy switchover` command when in nonstop switching mode



```
HP Switch(config)# redundancy switchover
A nonstop switching failover will occur; L2 operations will not be inter-
rupted. This management module will now reboot and will become the standby
module! You will need to use the other management module's console inter-
face. Do you want to continue [y/n]? y
This management module will now boot from the primary image and will
become the standby module! You will need to used the other management mod-
ule's console interface. Do you want to continue [y/n]? y

ROM information:
   Build directory: /sw/rom/build/bmrom(t2g)
   Build date:      Oct 15 2009
   Build time:      08:24:27
   Build version:   K.15.01
   Build number:    13040
Select profile (primary):

Booting Primary Software Image...
.
.
.

Standby Console>
```

Setting the active management module for next boot (CLI)

Syntax:

```
redundancy active-management [  management-module1 | management-module2
| standby  ]
```

The specified module becomes the active management module at the next system boot. This message displays:`On the next system boot, the module specified will become active.`

This command does not take effect if the standby management module has failed selftest.

`management-module1`	Configures management-module 1 as the active management module for the next system boot.
`management-module2`	Configures management-module 2 as the active management module for the next system boot.
`standby`	Configures the current standby module as the active management module for the next system boot if management module redundancy is enabled. If redundancy is disabled, it becomes enabled as a standby module at the next boot or failover event.

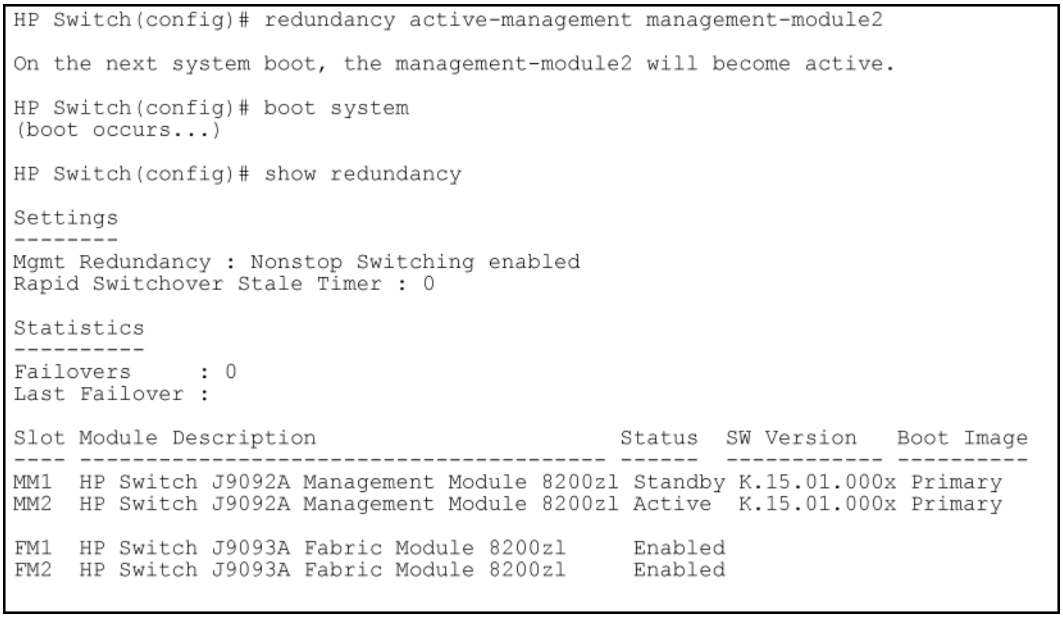
If the specified management module is not there or is in failed mode, this message displays:

```
The specified module is not present or is in failed state.
```

Example

Figure 114 (page 249) shows an example of setting **management module 2** to be the **active management module**.

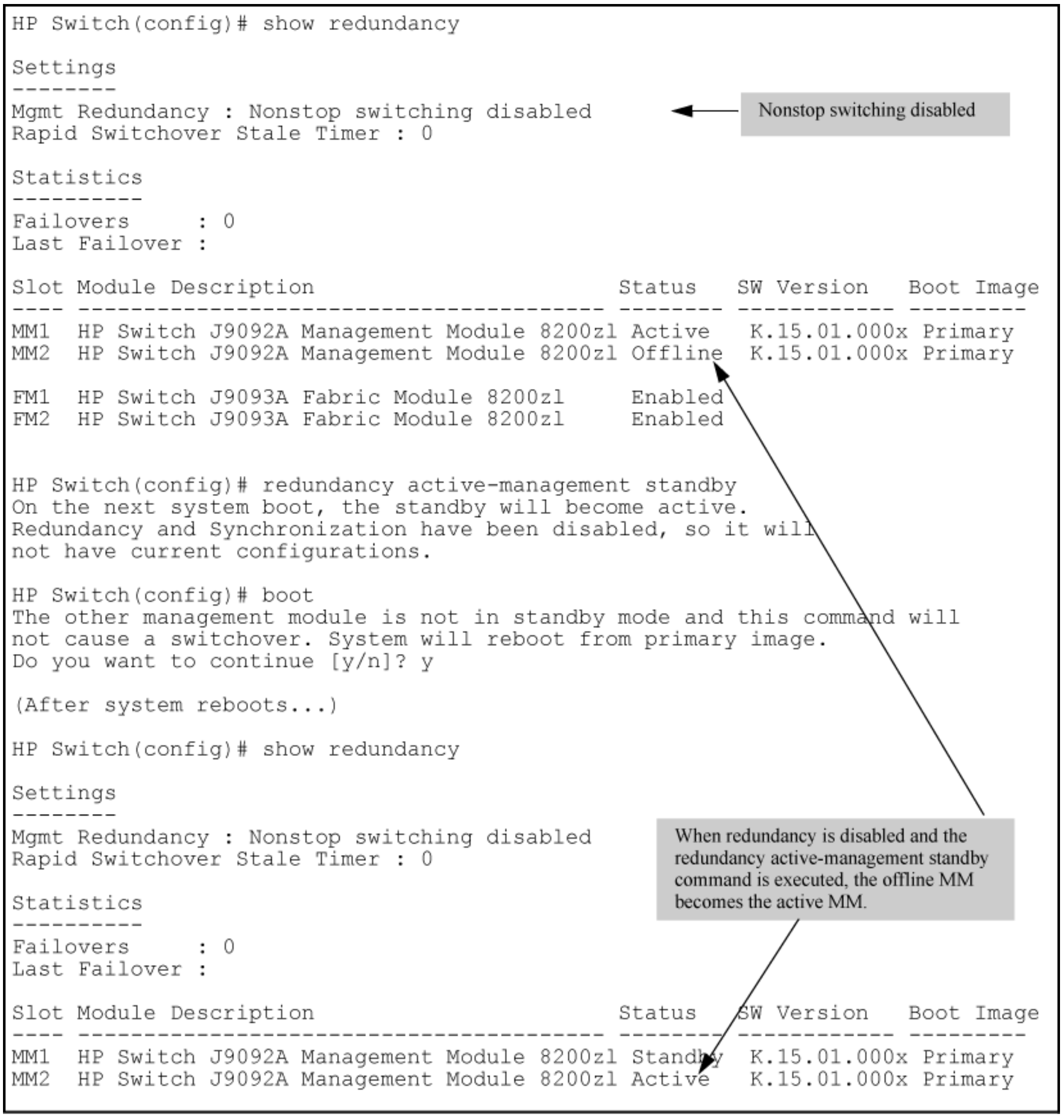
Figure 114 Setting a management module to be active on the next boot



```
HP Switch(config)# redundancy active-management management-module2

On the next system boot, the management-module2 will become active.

HP Switch(config)# boot system
(boot occurs...)

HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop Switching enabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                        Status  SW Version   Boot Image
---- ---------------------------------------- ------  ------------ ----------
MM1  HP Switch J9092A Management Module 8200zl Standby K.15.01.000x Primary
MM2  HP Switch J9092A Management Module 8200zl Active  K.15.01.000x Primary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Enabled
```

If management module redundancy has been disabled and you specify the standby module with the `active-management` command, upon rebooting, the offline module becomes the standby module. The state of redundancy (enabled or disabled) is based on the value in the configuration file in the offline (now standby) module. The configuration files have not been synchronized if management module redundancy has been disabled. An example of making the offline management module become the standby management module when **redundancy** is disabled is shown in Figure 115 (page 250).

Figure 115 Showing the results of switching to standby module when redundancy is disabled



```
HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop switching disabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                       Status   SW Version   Boot Image
---- ---------------------------------------- -------- ------------ ---------
MM1  HP Switch J9092A Management Module 8200zl Active   K.15.01.000x Primary
MM2  HP Switch J9092A Management Module 8200zl Offline  K.15.01.000x Primary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Enabled


HP Switch(config)# redundancy active-management standby
On the next system boot, the standby will become active.
Redundancy and Synchronization have been disabled, so it will
not have current configurations.

HP Switch(config)# boot
The other management module is not in standby mode and this command will
not cause a switchover. System will reboot from primary image.
Do you want to continue [y/n]? y

(After system reboots...)

HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop switching disabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                       Status   SW Version   Boot Image
---- ---------------------------------------- -------- ------------ ---------
MM1  HP Switch J9092A Management Module 8200zl Standby  K.15.01.000x Primary
MM2  HP Switch J9092A Management Module 8200zl Active   K.15.01.000x Primary
```

Nonstop switching disabled

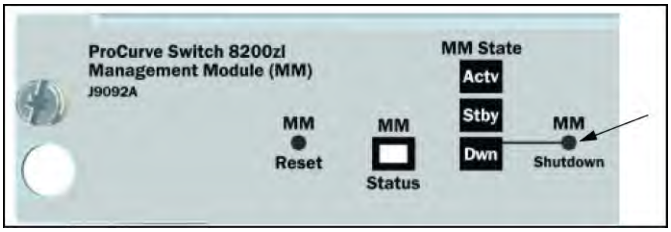
When redundancy is disabled and the redundancy active-management standby command is executed, the offline MM becomes the active MM.

Hotswapping out the active management module

For information about management module switchover and hotswapping management modules, see“Management module switchover” (page 268) and “About hotswapping out the active management module” (page 269).

1. On the management module to be hotswapped out, press the **MM Shutdown** button. It is located between the **Module Operation** and **Component Status** LEDs. (See Figure 116 (page 250).)

   Figure 116 The MM Shutdown button

2. The **Dwn** LED to the right of the **MM Shutdown** button begins flashing green. File synchronization will complete before shutdown occurs.

3. The standby module takes control and the switchover occurs. It is now the active management module.
4. The **Dwn** LED on the management module being hotswapped out turns green and all other LEDs go out when it is OK to remove the module.
5. The module being hotswapped out goes into offline mode. In the offline mode, the module cannot take over when the active module fails over.

NOTE: If you remove the active management module without pressing the **MM Shutdown** button, any files that may have been in the process of synchronizing will not finish synchronizing to the standby module and all file transfer is aborted.

For information about hotswapping in a management mode and software version mismatch between active and hotswapped modules, see "Hotswapping in a management module" (page 269) and "Software version mismatch between active and hotswapped module" (page 270).

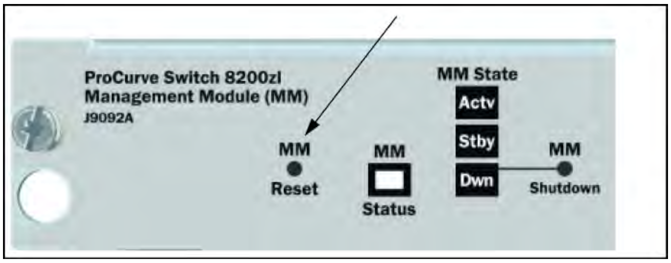
Resetting the management module

The **MM Reset** button, shown in Figure 117 (page 251), found on each management module reboots its management module. If the management module is active and management module redundancy is enabled, switchover occurs. The standby management module is notified immediately. It then takes over and becomes the active management module. If the **MM Reset** button is pressed on the standby management module, that module reboots but no other switch operations are affected. The active management module remains in control.

If management module redundancy is disabled, the active management module reboots and remains in control, as long as it passes selftest.

△ **CAUTION:** HP does not recommend using the **MM Reset** button to trigger a switchover. Files being copied over at the time of the reset will be aborted.

Figure 117 The MM Reset button on the 8200zl management module



For information about downloading a new software version, see "About downloading a new software version" (page 271).

For information about synchronizing files after downloading, see "File synchronization after downloading" (page 271).

For information about software version mismatches after downloading, see "Potential software version mismatches after downloading" (page 271).

Viewing management information

For information about active management module commands, see "Disable management module redundancy with only one module present" (page 274). The sections that follow provide information about the `show` commands that display various aspects of management information.

Syntax:

```
show modules [details]
```

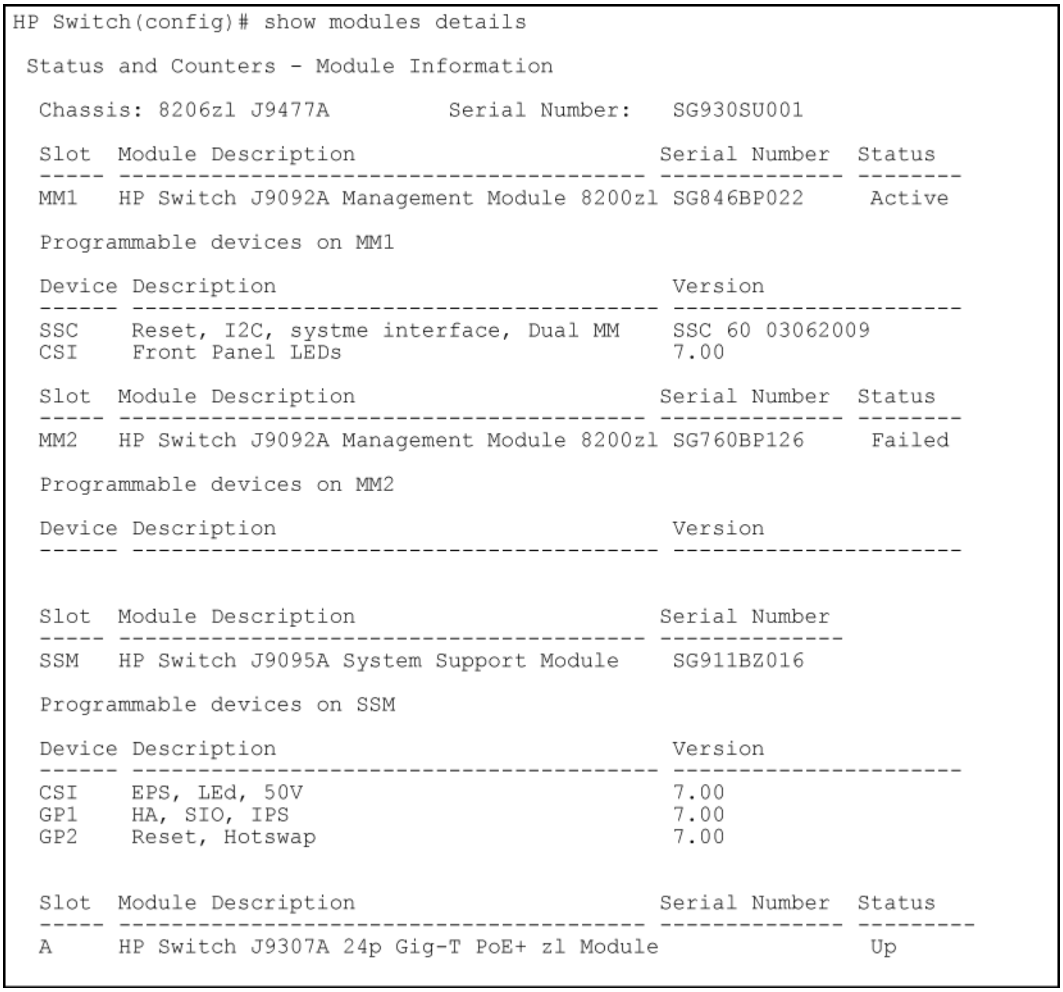
Displays information about the installed modules, including:

- The slot in which the module is installed
- The module description
- The serial number
- The status
- The System Support Module description, serial number, and status (8200zl switches only)

Additionally, the part number (J number) and serial number of the chassis is displayed.

Example

Figure 118 The `show modules details` command for the 8212zl showing SSM and mini-GBIC information



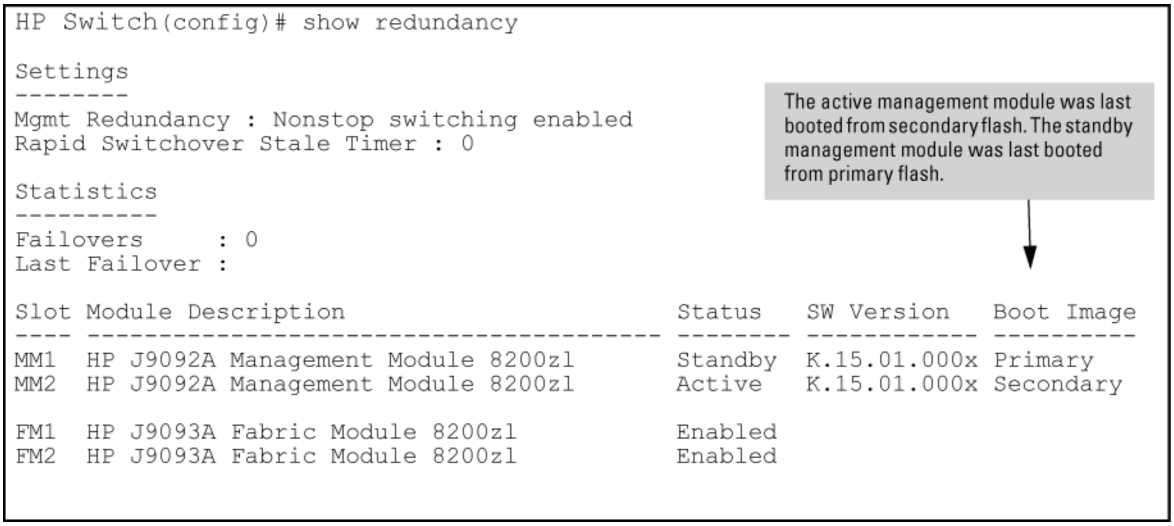
```
HP Switch(config)# show modules details

 Status and Counters - Module Information

  Chassis: 8206zl J9477A         Serial Number:   SG930SU001

  Slot  Module Description                       Serial Number  Status
  ----- ---------------------------------------- -------------- --------
  MM1   HP Switch J9092A Management Module 8200zl SG846BP022     Active

  Programmable devices on MM1

  Device Description                              Version
  ------ ---------------------------------------- ----------------------
  SSC    Reset, I2C, systme interface, Dual MM    SSC 60 03062009
  CSI    Front Panel LEDs                         7.00

  Slot  Module Description                       Serial Number  Status
  ----- ---------------------------------------- -------------- --------
  MM2   HP Switch J9092A Management Module 8200zl SG760BP126     Failed

  Programmable devices on MM2

  Device Description                              Version
  ------ ---------------------------------------- ----------------------


  Slot  Module Description                       Serial Number
  ----- ---------------------------------------- --------------
  SSM   HP Switch J9095A System Support Module    SG911BZ016

  Programmable devices on SSM

  Device Description                              Version
  ------ ---------------------------------------- ----------------------
  CSI    EPS, LEd, 50V                            7.00
  GP1    HA, SIO, IPS                             7.00
  GP2    Reset, Hotswap                           7.00


  Slot  Module Description                       Serial Number  Status
  ----- ---------------------------------------- -------------- ---------
  A     HP Switch J9307A 24p Gig-T PoE+ zl Module                Up
```

Viewing information about the management and fabric modules

The `show redundancy` command displays information about the management and fabric modules. It displays the flash image last booted from, even if the `boot set-default` command has been set to change the flash booted from on the next boot.

Example

Figure 119 `show redundancy` command



```
HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop switching enabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                            Status   SW Version   Boot Image
---- ------------------------------------------- -------- ------------ ----------
MM1  HP J9092A Management Module 8200zl            Standby  K.15.01.000x Primary
MM2  HP J9092A Management Module 8200zl            Active   K.15.01.000x Secondary

FM1  HP J9093A Fabric Module 8200zl                Enabled
FM2  HP J9093A Fabric Module 8200zl                Enabled
```

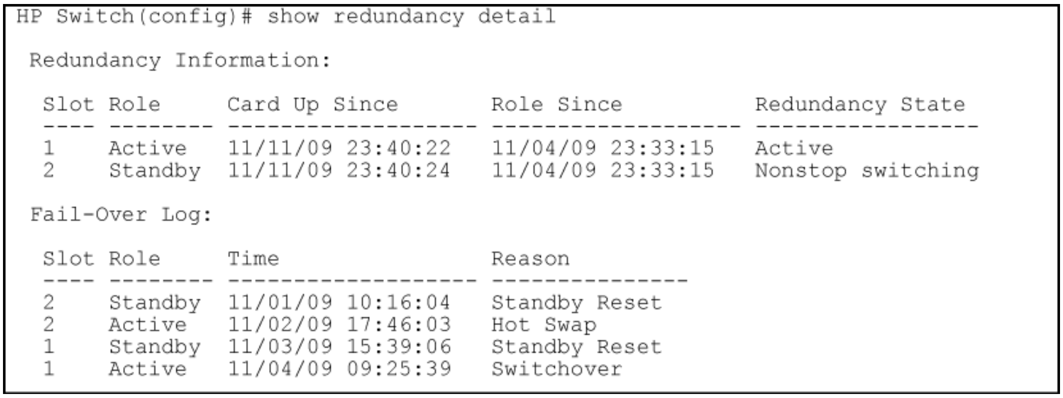
The active management module was last booted from secondary flash. The standby management module was last booted from primary flash.

Viewing information about the redundancy role of each management module

The `show redundancy` command with the `detail` option displays information about the redundancy role of each management module, as well as statistical information such as how long the module has been up.

Example

Figure 120 `show redundancy detail` command



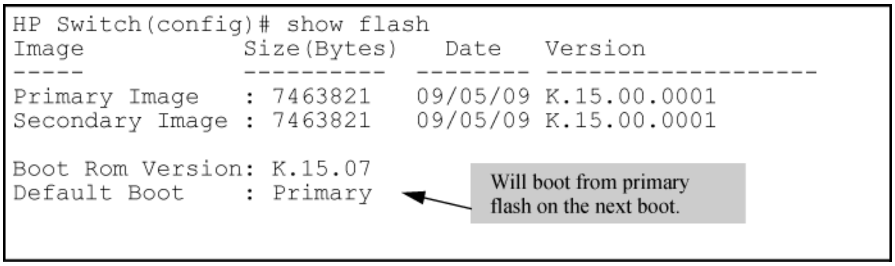
```
HP Switch(config)# show redundancy detail

 Redundancy Information:

  Slot Role     Card Up Since        Role Since           Redundancy State
  ---- -------- -------------------- -------------------- -----------------
  1    Active   11/11/09 23:40:22    11/04/09 23:33:15    Active
  2    Standby  11/11/09 23:40:24    11/04/09 23:33:15    Nonstop switching

 Fail-Over Log:

  Slot Role     Time                 Reason
  ---- -------- -------------------- ---------------
  2    Standby  11/01/09 10:16:04    Standby Reset
  2    Active   11/02/09 17:46:03    Hot Swap
  1    Standby  11/03/09 15:39:06    Standby Reset
  1    Active   11/04/09 09:25:39    Switchover
```

Viewing which software version is in each flash image

The `show flash` command displays which software version is in each flash image. The **Default Boot** field displays which flash image will be used for the next boot.

Example

Figure 121 `show flash` command



```
HP Switch(config)# show flash
Image               Size(Bytes)   Date     Version
-----               ----------- -------- -------------------
Primary Image     : 7463821    09/05/09 K.15.00.0001
Secondary Image : 7463821    09/05/09 K.15.00.0001

Boot Rom Version: K.15.07
Default Boot     : Primary
```

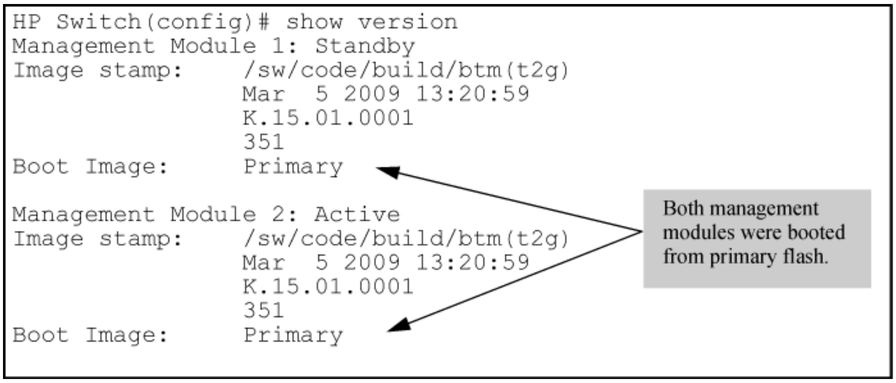
Will boot from primary flash on the next boot.

Viewing system software image information for both management modules

The `show version` command displays system software image information for both management modules, as well as which module is the active management module and which is the standby management module. The Boot Image field displays which flash image last booted from, even if the `boot set-default` command has been set to change the flash booted from on the next boot. The output of the `show version` command when redundancy is enabled is shown in Figure 122 (page 254).

Example

Figure 122 `show version` command when redundancy is enabled



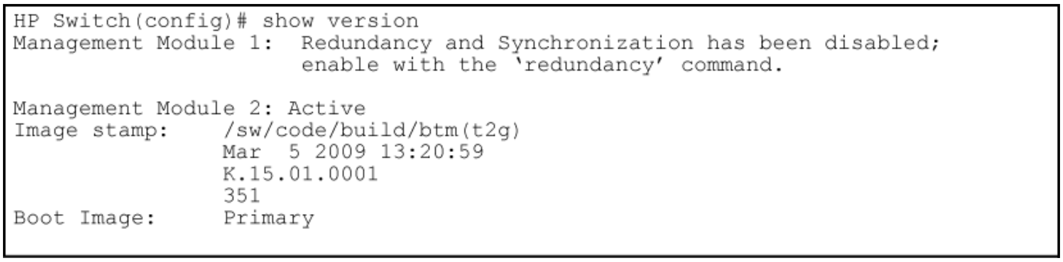
```
HP Switch(config)# show version
Management Module 1: Standby
Image stamp:     /sw/code/build/btm(t2g)
                 Mar  5 2009 13:20:59
                 K.15.01.0001
                 351
Boot Image:      Primary

Management Module 2: Active
Image stamp:     /sw/code/build/btm(t2g)
                 Mar  5 2009 13:20:59
                 K.15.01.0001
                 351
Boot Image:      Primary
```

Both management modules were booted from primary flash.

When redundancy is disabled, the output of the `show version` command changes, as shown in Figure 123 (page 254).

Example

Figure 123 `show version` command when redundancy is disabled



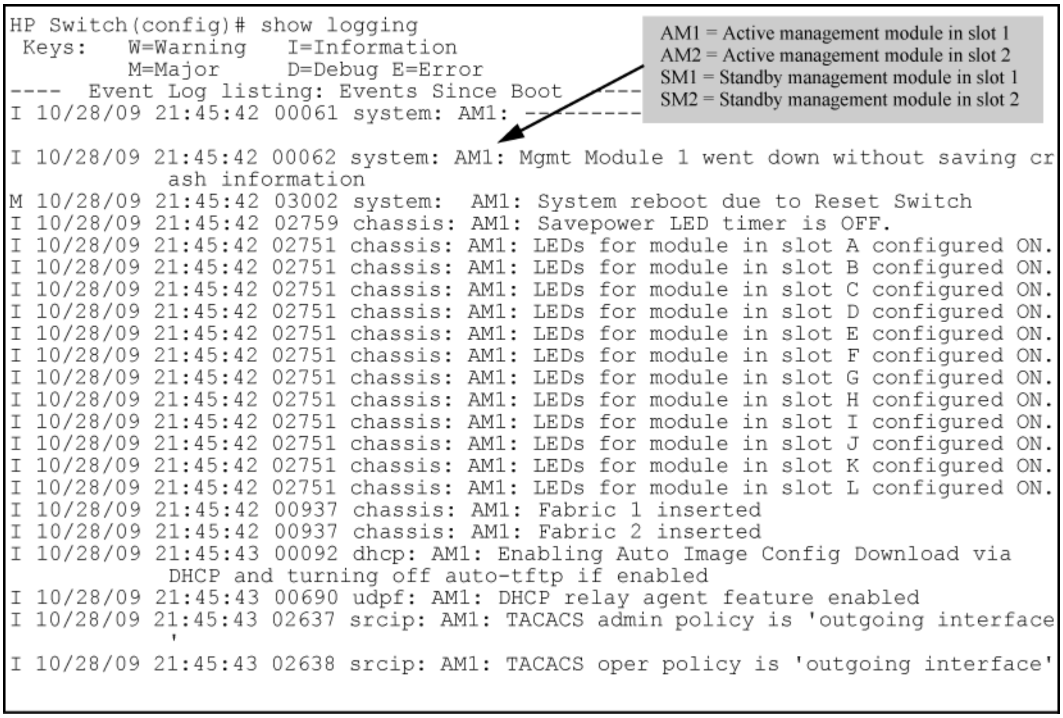
```
HP Switch(config)# show version
Management Module 1:  Redundancy and Synchronization has been disabled;
                      enable with the 'redundancy' command.

Management Module 2: Active
Image stamp:     /sw/code/build/btm(t2g)
                 Mar  5 2009 13:20:59
                 K.15.01.0001
                 351
Boot Image:      Primary
```

Viewing the status of the switch and its management modules

The `show logging` command displays the status of the switch and its management modules. See "Displaying module events" (page 258). To show log messages in reverse chronological order (most recent messages displayed first), enter `show log -r`.

Example

Figure 124 `show log` command output



```
HP Switch(config)# show logging
 Keys:   W=Warning   I=Information
         M=Major     D=Debug E=Error
----  Event Log listing: Events Since Boot ----
I 10/28/09 21:45:42 00061 system: AM1: ----------

I 10/28/09 21:45:42 00062 system: AM1: Mgmt Module 1 went down without saving cr
            ash information
M 10/28/09 21:45:42 03002 system:  AM1: System reboot due to Reset Switch
I 10/28/09 21:45:42 02759 chassis: AM1: Savepower LED timer is OFF.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot A configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot B configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot C configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot D configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot E configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot F configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot G configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot H configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot I configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot J configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot K configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot L configured ON.
I 10/28/09 21:45:42 00937 chassis: AM1: Fabric 1 inserted
I 10/28/09 21:45:42 00937 chassis: AM1: Fabric 2 inserted
I 10/28/09 21:45:43 00092 dhcp: AM1: Enabling Auto Image Config Download via
            DHCP and turning off auto-tftp if enabled
I 10/28/09 21:45:43 00690 udpf: AM1: DHCP relay agent feature enabled
I 10/28/09 21:45:43 02637 srcip: AM1: TACACS admin policy is 'outgoing interface
            '
I 10/28/09 21:45:43 02638 srcip: AM1: TACACS oper policy is 'outgoing interface'
```

AM1 = Active management module in slot 1
AM2 = Active management module in slot 2
SM1 = Standby management module in slot 1
SM2 = Standby management module in slot 2

Standby management module commands

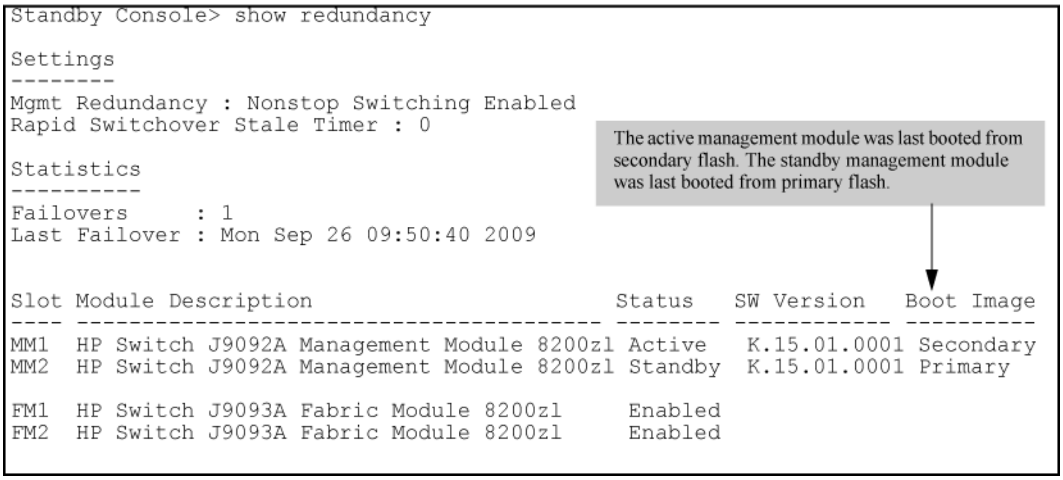
The standby management module, by design, has very little console capability. You can use three commands—`show flash`, `show version`, and `show redundancy`. The `show redundancy` command displays when a management module is in standby mode.

Viewing redundancy status on the standby module (CLI)

Use the `show redundancy` command to display redundancy status on the standby module, as shown in Figure 125 (page 255). This command displays the flash image last booted from, even if the `boot set-default` command has been set to change the flash booted from on the next boot.

Example

Figure 125 `show redundancy` command for standby module



```
Standby Console> show redundancy

Settings
--------
Mgmt Redundancy : Nonstop Switching Enabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers      : 1
Last Failover : Mon Sep 26 09:50:40 2009


Slot Module Description                          Status    SW Version    Boot Image
---- ----------------------------------------  --------  ------------  ----------
MM1  HP Switch J9092A Management Module 8200zl Active    K.15.01.0001 Secondary
MM2  HP Switch J9092A Management Module 8200zl Standby   K.15.01.0001 Primary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Enabled
```

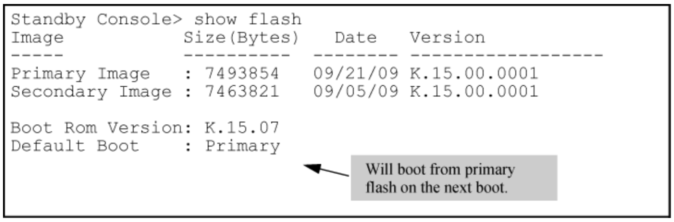
The active management module was last booted from secondary flash. The standby management module was last booted from primary flash.

Viewing the flash information on the standby module (CLI)

Use the `show flash` command to display the flash information on the standby module, as shown in Figure 126 (page 256). The **Default Boot** field displays which **flash image** will be used for the next boot.

Example

Figure 126 `show flash` command for standby module



```
Standby Console> show flash
Image           Size(Bytes)   Date    Version
-----           ----------  -------- ------------------
Primary Image   : 7493854   09/21/09 K.15.00.0001
Secondary Image : 7463821   09/05/09 K.15.00.0001

Boot Rom Version: K.15.07
Default Boot    : Primary
```

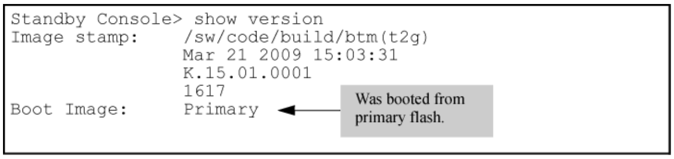
Will boot from primary flash on the next boot.

Viewing the version information on the standby module (CLI)

Use the `show version` command to display the version information on the standby module, as shown in Figure 127 (page 256). The **Boot Image** field displays which flash image was last booted from, even if the `boot set-default` command has been set to change the flash booted from on the next boot. Unlike executing the `show version` command on an active management module, this command shows only the running version of software on the standby management module.

Example

Figure 127 `show version` command for standby module



```
Standby Console> show version
Image stamp:    /sw/code/build/btm(t2g)
                Mar 21 2009 15:03:31
                K.15.01.0001
                1617
Boot Image:     Primary
```

Was booted from primary flash.

Setting the default flash for boot (CLI)

For more information about the boot command, see "CLI commands affected by redundant management" (page 274).

You can set which flash image to boot from as the default image on boot by using this command:

Syntax:

```
boot set-default flash[  primary | secondary  ]
```

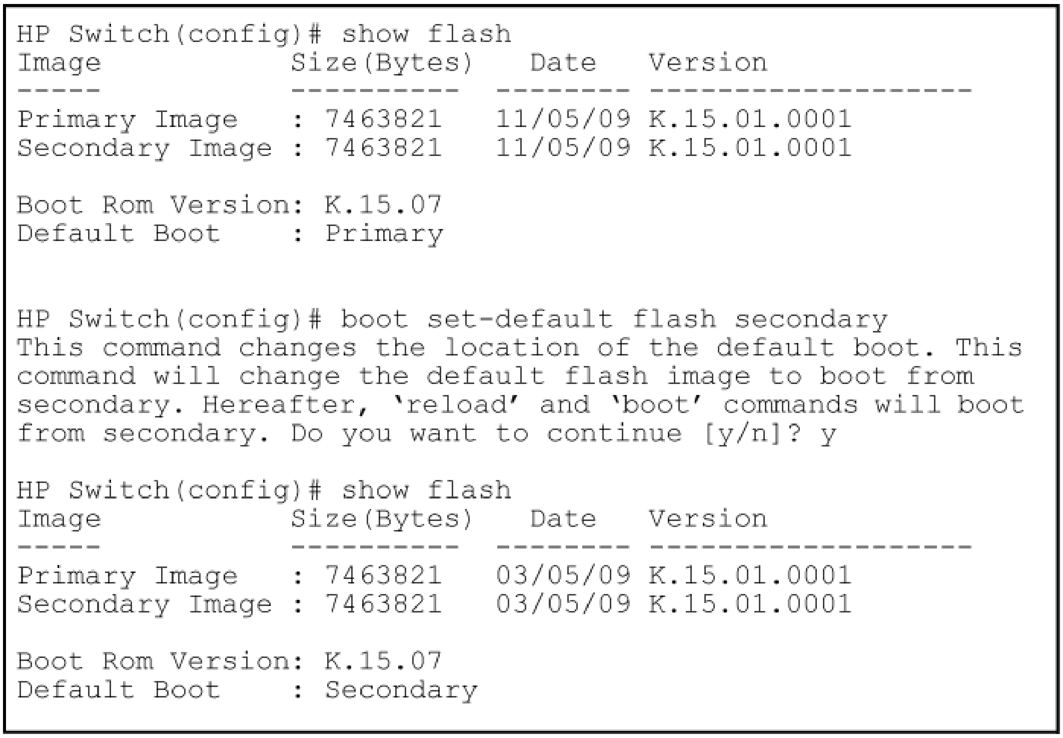
Sets the flash image to boot from on the next boot.

`primary`	Boots the primary flash image.
`secondary`	Boots the secondary flash image.

Example

Figure 128 (page 257) shows an example of the output when the command is used to set the boot default to secondary flash.

Figure 128 `boot set-default` **command defaulting to secondary flash**



```
HP Switch(config)# show flash
Image              Size(Bytes)   Date     Version
-----              ----------  -------- -------------------
Primary Image    : 7463821     11/05/09 K.15.01.0001
Secondary Image  : 7463821     11/05/09 K.15.01.0001

Boot Rom Version: K.15.07
Default Boot    : Primary


HP Switch(config)# boot set-default flash secondary
This command changes the location of the default boot. This
command will change the default flash image to boot from
secondary. Hereafter, 'reload' and 'boot' commands will boot
from secondary. Do you want to continue [y/n]? y

HP Switch(config)# show flash
Image              Size(Bytes)   Date     Version
-----              ----------  -------- -------------------
Primary Image    : 7463821     03/05/09 K.15.01.0001
Secondary Image  : 7463821     03/05/09 K.15.01.0001

Boot Rom Version: K.15.07
Default Boot    : Secondary
```

Booting the active management module from the current default flash (CLI)

Use the `reload` command to boot the active management module from the current default flash (You can change the default flash with the `boot set-default` command. See “Setting the default flash for boot (CLI)” (page 256)). Switchover occurs if redundancy is enabled and the standby management module is in standby mode. If redundancy is disabled or the standby management module is not present, the `reload` command boots the system.

NOTE: The `reload` command is a "warm" reboot; it skips the Power on Self Test routine.

Syntax:

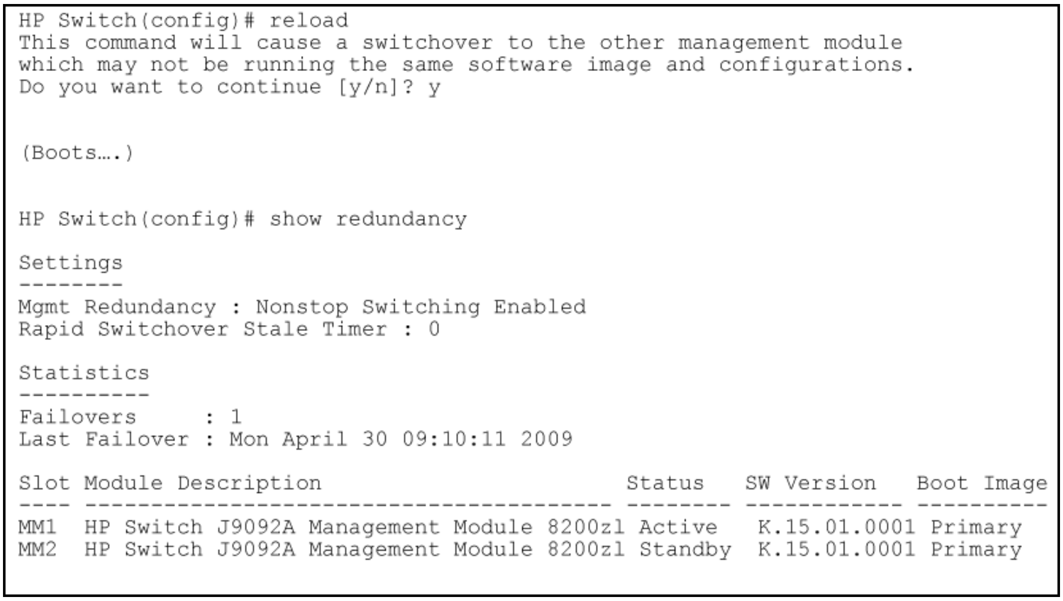
`reload <cr>`

Boots (warm reboot) the active management module. Switchover to the standby management module occurs if `management module` redundancy is enabled. If redundancy is disabled or if there is no standby management module, the `reload` command boots the system.

NOTE: If the `running config` file is different from the stored config file, you are prompted to save the config file. The `reload at/after` versions of this command do not display a prompt to save configuration file changes: the changes are lost on the scheduled reload.

Example

Figure 129 `reload` command with redundancy enabled



```
HP Switch(config)# reload
This command will cause a switchover to the other management module
which may not be running the same software image and configurations.
Do you want to continue [y/n]? y


(Boots….)


HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop Switching Enabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 1
Last Failover : Mon April 30 09:10:11 2009

Slot Module Description                       Status   SW Version   Boot Image
---- ---------------------------------------- -------- ------------ ----------
MM1  HP Switch J9092A Management Module 8200zl Active   K.15.01.0001 Primary
MM2  HP Switch J9092A Management Module 8200zl Standby  K.15.01.0001 Primary
```

For information on other commands that are affected by redundant management, see "Additional commands affected by redundant management" (page 277).

Displaying module events

Viewing log events (CLI)

The log file displays messages about the activities and status of the management modules. Enter this command to display the messages:

Syntax:

`show logging [ -a, -b, -r, -s, -t, -m, -p, -w, -i, -d,  `*`option-str`*`  ]`

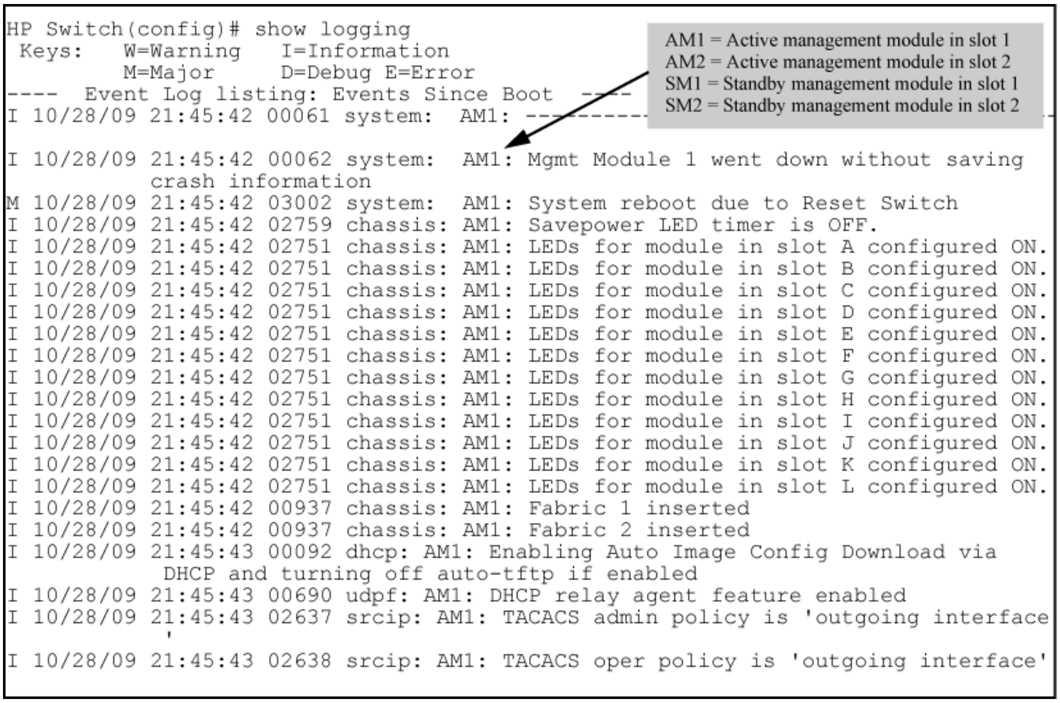
Displays log events.

The event messages are tagged with the management module state and the management module slot (AM1 or AM2, SM1 or SM2). Synchronization is maintained by syncing the standby management module log events with the active management module. In this way, events are available for both management modules. Only the active management module events are shown unless you select the `-s` option. This option works like the `-a` option, except that the events for both the active management module and standby management module are displayed.

For more information on command options available with the `show logging` command, see "CLI: Displaying the Event Log" in the "Troubleshooting" chapter of this guide.

Example

Figure 130 Log file listing



```
HP Switch(config)# show logging
 Keys:    W=Warning    I=Information
          M=Major      D=Debug E=Error
----  Event Log listing: Events Since Boot  ----
I 10/28/09 21:45:42 00061 system:  AM1: ---------

I 10/28/09 21:45:42 00062 system:  AM1: Mgmt Module 1 went down without saving
           crash information
M 10/28/09 21:45:42 03002 system:  AM1: System reboot due to Reset Switch
I 10/28/09 21:45:42 02759 chassis: AM1: Savepower LED timer is OFF.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot A configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot B configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot C configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot D configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot E configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot F configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot G configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot H configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot I configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot J configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot K configured ON.
I 10/28/09 21:45:42 02751 chassis: AM1: LEDs for module in slot L configured ON.
I 10/28/09 21:45:42 00937 chassis: AM1: Fabric 1 inserted
I 10/28/09 21:45:42 00937 chassis: AM1: Fabric 2 inserted
I 10/28/09 21:45:43 00092 dhcp: AM1: Enabling Auto Image Config Download via
            DHCP and turning off auto-tftp if enabled
I 10/28/09 21:45:43 00690 udpf: AM1: DHCP relay agent feature enabled
I 10/28/09 21:45:43 02637 srcip: AM1: TACACS admin policy is 'outgoing interface
            '
I 10/28/09 21:45:43 02638 srcip: AM1: TACACS oper policy is 'outgoing interface'
```

AM1 = Active management module in slot 1
AM2 = Active management module in slot 2
SM1 = Standby management module in slot 1
SM2 = Standby management module in slot 2

Copying crash file information to another file (CLI)

Crash logs for all modules are always available on the active management module. You can use the `copy crash-log` and `copy crash-data` commands to copy the information to a file of your choice.

Syntax:

`copy crash-log [ *slot-id* | mm ] tftp *ip-address filename*`

Copies the crash logs of both the active and standby management modules to a user-specified file. If no parameter is specified, files from all modules (management and interface) are concatenated.

`slot-id`	Retrieves the crash log from the module in the specified slot.
`mm`	Retrieves the crash logs from both management modules and concatenates them.

Syntax:

`copy crash-data [ *slot-id* | mm ] tftp *ip-address filename*`

Copies the crash data of both the active and standby management modules to a user-specified file. If no parameter is specified, files from all modules (management and interface) are concatenated.

`slot-id`	Retrieves the crash data from the module in the specified slot.
`mm`	Retrieves the crash data from both management modules and concatenates them.

Viewing saved crash information

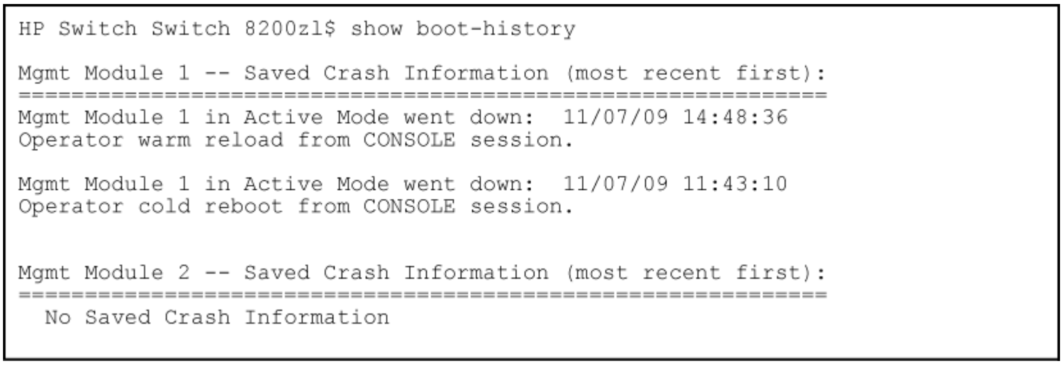
Syntax:

`show boot-history`

Displays the system boot log.

Example

Figure 131 The system boot log file



```
HP Switch Switch 8200zl$ show boot-history

Mgmt Module 1 -- Saved Crash Information (most recent first):
=============================================================
Mgmt Module 1 in Active Mode went down:  11/07/09 14:48:36
Operator warm reload from CONSOLE session.

Mgmt Module 1 in Active Mode went down:  11/07/09 11:43:10
Operator cold reboot from CONSOLE session.


Mgmt Module 2 -- Saved Crash Information (most recent first):
=============================================================
  No Saved Crash Information
```

Enabling and disabling fabric modules (CLI)

The fabric modules can be enabled or disabled even if they are not present in the switch. You cannot disable both fabric modules at the same time; one must be enabled.

Use this command to enable or disable the redundant fabric modules. Disabling one fabric module reduces the overall switching capacity of the 8200zl series switches. On some networks where network utilization is less than 50%, you may not notice any degradation of performance.

Syntax:

`redundancy fabric-module[ 1 | 2 ][ enable | disable ]`

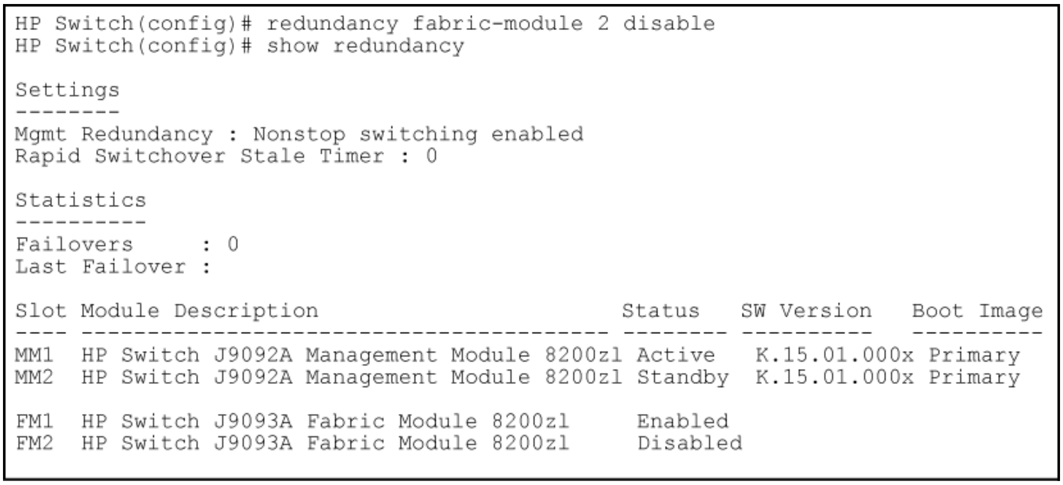
Allows enabling or disabling of fabric modules. (You cannot have both fabric modules disabled at the same time.)

Default: Both fabric modules are enabled.

NOTE: The redundant fabric modules do not support nonstop switching.

Example

Figure 132 Disabling a fabric module



```
HP Switch(config)# redundancy fabric-module 2 disable
HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop switching enabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                       Status   SW Version   Boot Image
---- ---------------------------------------- -------- ----------   ----------
MM1  HP Switch J9092A Management Module 8200zl Active   K.15.01.000x Primary
MM2  HP Switch J9092A Management Module 8200zl Standby  K.15.01.000x Primary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Disabled
```

Overview of chassis redundancy (8200zl switches)

The HP 8200zl switches provide high availability through the use of hot-swappable, redundant management modules. In the event of a failure on the active management module, management module redundancy allows a quick and unattended transition from the active management module to the standby management module. The standby management module now becomes the active management module. Management module redundancy keeps the switch operating and reduces network downtime.

The advantages of redundant management are:

- Maintaining switch operation if a hardware failure occurs on the active management module
- Minimizing restart time caused by the failure of a management module
- Hotswapping a failed management module with no downtime

Nonstop switching with redundant management modules

Beginning with software version K.15.01, you can use either nonstop switching or warm-standby redundant management.

The advantages of nonstop switching are:

- Quick, seamless transition to the standby management module; no reboot is necessary
- Switching of packets continues without interruption

How the management modules interact

When the switch boots up, the management modules run selftest to decide which is the active module and which is the standby module (see "Notes on how the active module is determined" (page 279)). The module that becomes active finishes booting and then brings up the interface modules and ports.

If you are using nonstop switching mode, the standby management module is synced continuously with the active management module so that all features and config files are the same on both management modules. The standby management module is ready to become the active management module. If the active management module fails or if there is a manual switchover, switching continues without interruption.

If you are using warm-standby mode, the standby module boots to a certain point, syncs basic files such as the config and security files, and finishes booting only if the active management module fails or you choose to change which module is the active module.

The two management modules communicate by sending heartbeats back and forth.

About using redundant management

The CLI commands for redundant management are shown at the beginning of the chapter. Additionally, some other commands are affected by redundant management (See "CLI commands affected by redundant management" (page 274)).

Transition from no redundancy to nonstop switching

While the switch is transitioning from no redundancy mode to nonstop switching mode, no configuration changes are allowed. The management modules are syncing information during the transition period.

About setting the rapid switchover stale timer

After a failover has occurred, use the rapid switchover stale timer to set the amount of time that you want route and neighbor table entries to be re-added to the FIB on the active management module.

Layer 3 applications and protocols rely on existing routing information in the FIB. They restart and operate as if the switch performed a quick reset.

When a failover occurs, the interface modules and the fabric modules continue forwarding Layer 3 traffic based on the information in the FIB. The transitioning standby management module marks all routes in the FIB as "stale". The routing protocols restart, reestablish their neighbors and reconverge. As a route is added in again, the route's stale designation is removed. After the rapid switchover stale timer expires, the remaining stale route entries are removed. Multicast flows are also removed; the multicast application re-adds the flows after failover completes.

About directing the standby module to become active

To make the standby management module become the active management module, use the `redundancy switchover` command. The switch will switchover after all files have finished synchronizing.

In nonstop switching mode:

- The switchover occurs quickly and seamlessly; no reboot is needed.
- There is no interruption in switching operations.

In warm-standby mode:

- The switchover may take several minutes if there have been recent configuration file changes or if you have downloaded a new operating system.
- The standby module finishes booting and becomes the active module.

The formerly active module becomes the standby module if it passes selftest.

Nonstop switching with VRRP

When Nonstop VRRP is enabled, VRRP continues to operate in its current state when a failover from the AMM to the SMM occurs. This provides an additional layer of redundancy in a switched network. VRRP state information is maintained between MMs so that VRRP operations resume immediately after failover from the AMM to SMM. Because of this quick resumption of operations there is no failover to the backup VRRP router in the network. The Master VRRP router continues to be active and operate as is.

The command for enabling Nonstop mode for VRRP must be executed in VRRP context. For more information on enabling and configuring VRRP, see "Steps for Provisioning VRRP Operation" on page 5-12 of the Multicast and Routing Guide for your switch.

Syntax:

```
(vrrp#) [no]
nonstop
```

Enabling Nonstop VRRP allows the VRRP router to retain control of IP addresses when the AMM fails over. The VRRP Backup router does not take control of the virtual IP addresses on the network.

The no version of the command disables Nonstop VRRP.

When Nonstop behavior is disabled, failure of the AMM on the VRRP Master results in the VRRP Backup router taking control of the virtual IP addresses on the network.

The commands must be executed in VRRP context.

NOTE: Before this command is executed, the command `redundancy management nonstop-switching` should be configured. Any prerequisites required for VRRP configuration commands, such as IP routing being enabled, remain as required prerequisites.

Default: Disabled

Example

Example 51 Example of enabling nonstop switching for VRRP and then displaying the output

This example shows nonstop VRRP being enabled. The `show vrrp config` command output displays the enabled status (see bold line below).

```
HP Switch(vlan-10-vrid-1)# nonstop
HP Switch(vlan-10-vrid-1)# show vrrp config

VRRP Global Configuration Information

VRRP Enabled  : Yes
Traps Enabled : Yes
Virtual Routers Respond to Ping Requests : Yes
VRRP Nonstop Enabled: Yes

VRRP Virtual Router Configuration Information

Vlan ID : 10
Virtual Router ID : 1

Administrative Status [Disabled] : Enabled
Mode [Uninitialized] : Backup
Priority [100] : 150
Advertisement Interval [1] : 1
Preempt Mode [True] : True
Preempt delay time : 0
Respond to Virtual IP Ping Requests [Yes] : Yes
Primary IP Address : Lowest

IP Address      Subnet Mask
--------------- ---------------
10.0.202.87     255.255.0.0
```

Example nonstop routing configuration

Example 52 Example of configuring the owner routing switch

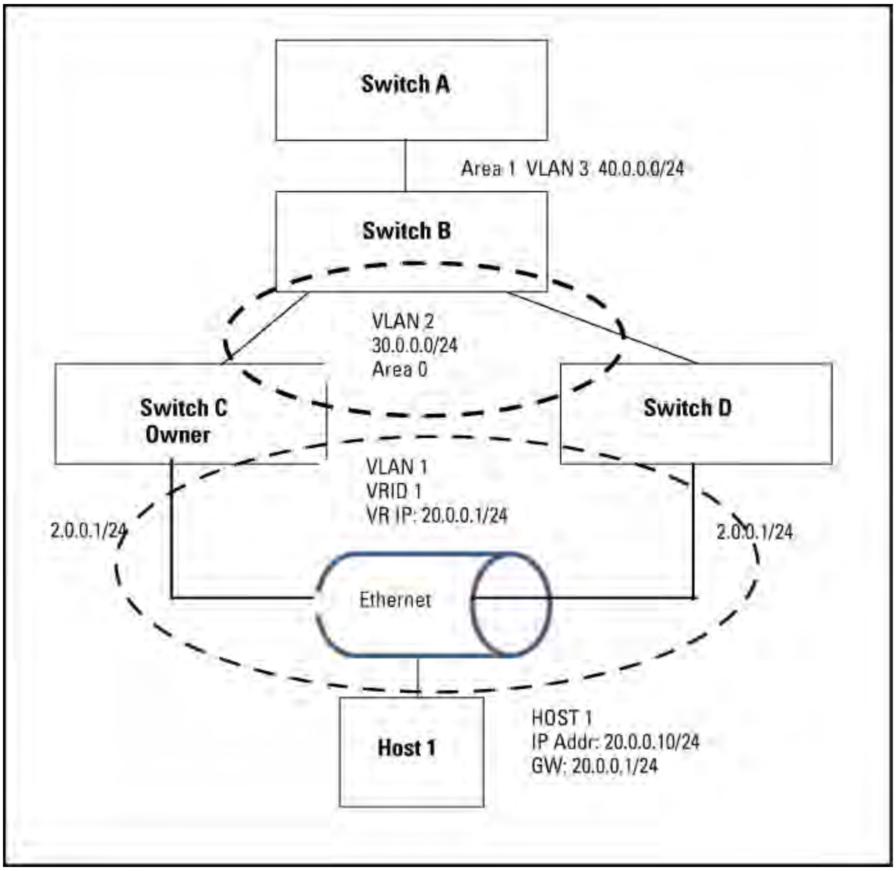
```
HP Switch C(config)# ip routing
HP Switch C(config)# router vrrp
HP Switch C(vrrp)# enable
HP Switch C(vrrp)# vlan 201
HP Switch C(vlan-201)# untag a1-a10
HP Switch C(vlan-201)# ip address 20.0.0.1/24
HP Switch C(vlan-201)# vrrp vrid 1
HP Switch C(vlan-201-vrid-1)# owner
HP Switch C(vlan-201-vrid-1)# virtual-ip-address 20.0.0.1/24
HP Switch C(vlan-201-vrid-1)# enable
```

Example 53 Example of configuring the backup routing switch

```
HP Switch D(config)# ip routing
HP Switch D(config)# router vrrp
HP Switch D(vrrp)# enable
HP Switch D(vrrp)# vlan 201
HP Switch D(vlan-201)# untag a1-a10
HP Switch D(vlan-201)# ip address 20.0.0.2/24
HP Switch D(vlan-201)# vrrp vrid 1
HP Switch D(vlan-201-vrid-1)# backup
HP Switch D(vlan-201-vrid-1)# virtual-ip-address 2.1.1.1/24
HP Switch D(vlan-201-vrid-1)# enable
```

The configuration is shown graphically in Figure 133 (page 265).

Figure 133 Example of nonstop routing configuration



Nonstop forwarding with RIP

On a Nonstop RIP router, the traffic does not get re-routed when the MM fails over. A request packet is sent on failover that asks for the router's peers to send routing updates to the requesting router. There is no loss of routed traffic.

Nonstop forwarding with OSPFv2 and OSPFv3

On a Nonstop OSPFv2 router, failover of a MM does not result in the OSPF v2 router being removed from the OSPFv2 domain. A restart request is sent by the Nonstop OSPFv2 router to the neighboring OSPFv2 routers, after which the graceful restart process begins. This behavior applies to OSPFv3 as well.

A graceful restart allows an OSPF routing switch to stay on the forwarding path while being restarted. The routing switch sends "grace LSAs" that notify its neighbors that it intends to perform a graceful restart. During the configurable grace period, the restarting switch's neighbors continue to announce the routing switch in their LSAs as long as the network topology remains unchanged. The neighbors run in "helper mode" while the routing switch restarts.

Graceful restart will fail under these conditions:

- There is a topology change during the graceful restart period. The helper switches exit helper mode and adjacencies are lost until the restarting switch rebuilds the adjacencies.
- The neighbor switches do not support helper mode.

For more information on OSPFv2 and OSPFv3 graceful restart, see RFC 3623 and RFC 5187.

Enabling nonstop forwarding for OSPFv2

The routing switch must be in ospf context when enabling Nonstop forwarding for OSPFv2. To enable Nonstop forwarding, enter this command.

Syntax:

```
(ospf)# [no]
nonstop
```

Enables nonstop forwarding for OSPFv2.

The no version of the command disables nonstop forwarding.

The commands must be executed in `ospf` context.

Default: Disabled

Example 54 Example of enabling nonstop forwarding for OSPFv2

```
HP Switch(ospf)# nonstop
```

Configuring restart parameters for OSPFv2

Syntax:

```
(ospf)# [no]
restart interval 1-1800 [strict-lsa-checking]
```

Specify the graceful restart timeout interval in seconds.

The no version of the command sets the restart parameters to the default values.

Default: Disabled

`interval 1–1800`

The graceful restart timeout interval (grace period) in seconds. Default: 120 seconds

`strict-lsa-checking`

Used in OSFPv2 context to enable or disable strict LSA operation in a network segment for a neighboring router that is attempting a graceful restart. When enabled, this operation halts Helper mode support if a change in LSAs (topology change) is detected during the neighbor’s restart period.

The no form of this command disables strict LSA operation.

Default: Strict LSA operation enabled

Viewing OSPFv2 nonstop forwarding information

To display the status of Nonstop forwarding information, enter the `show ip ospf general` command.

Example 55 Example of output showing status of nonstop forwarding for OSPFv2

```
HP Switch(config)# show ip ospf general

OSPF General Status

OSPF protocol  :enabled
Router ID      :10.10.10.80
.
.
.
Nonstop forwarding : Enabled
Graceful Restart Interval : 500
Graceful Restart Helper Mode : Enabled
.
.
.
```

Enabling nonstop forwarding for OSPFv3

The routing switch must be in `ospf3` context when enabling Nonstop forwarding for OSPFv3. To enable nonstop forwarding, enter this command.

Syntax:

`(ospf3)#` [no]
`nonstop`

Enables nonstop forwarding for OSPFv3.

The no version of the command disables nonstop forwarding.

The commands must be executed in `ospf3` context.

Default: Disabled

Example 56 Example of enabling nonstop forwarding for OSPFv3

```
HP Switch(ospf3)# nonstop
```

Configuring restart parameters for OSPFv3

Syntax:

`(ospf3)#` [no]
`restart interval 1-1800 [strict-lsa-checking`]

Specify the graceful restart timeout interval in seconds.

The no version of the command sets the restart parameters to the default values. Default: Disabled

`interval 1-1800`

The graceful restart timeout interval (grace period) in seconds. Default: 120 seconds

`strict-lsa-checking`

Used in OSFPv3 context to enable or disable strict LSA operation in a network segment for a neighboring router that is attempting a graceful restart. When enabled, this operation halts Helper mode support if a change in LSAs (topology change) is detected during the neighbor’s restart period.

The no form of this command disables strict LSA operation.

Default: Strict LSA operation enabled

Viewing OSPFv3 nonstop forwarding information

To display the status of Nonstop forwarding information, enter the `show ipv6 ospf3 general` command.

Example 57 Example of output showing status of nonstop forwarding for OSPFv3

```
HP Switch(config)# show ipv6 ospf3 general

OSPFv3 General Status

 OSPFv3 protocol  :enabled
 Router ID      :10.10.10.80
.
.
.
 Nonstop forwarding : Enabled
 Graceful Restart Interval : 500
 Graceful Restart Helper Mode : Enabled
.
.
.
```

Hotswapping management modules

Management module switchover

Events that cause a switchover

There are a number of events that can cause the active management module to switchover to the standby management module when management module redundancy is enabled:

- The active management module crashes
- The standby management module does not receive a heartbeat from the active management module
- The `redundancy switchover` command is executed
- The **MM Reset** button on the active management module is pressed
- The **MM Shutdown** button on the active management module is pressed
- The `boot` or `boot active` command is executed
- The `reload` command is executed
- There is a hardware failure on the active management module

In all of these cases, the standby management module takes control and performs the actual switchover. The reason for the switchover is entered in log messages on the newly active management module and to any configured Syslog servers.

What happens when switchover occurs

When a switchover occurs, the features that support nonstop switching continue to operate in an uninterrupted manner. See "Nonstop switching features" (page 281) for a list of the supported features.

The features that do not support nonstop switching perform as if the switch had just finished booting; however, no actual boot time occurs.

NOTE:
When meshing configuration changes are made on a redundant management system, you must execute `write mem` and then the `boot system` command to boot *both* management modules for the changes to be activated.

Meshing is not supported by nonstop switching.

NOTE:
If the switch is a querier and a failover occurs, the querier continues to be the same on the standby management module; no new querier election process occurs on the standby management module.

When switchover will not occur

There are some events for which a switchover is not triggered:

- When a `boot system` command is executed
- When the **Clear** button on the System Support module is pressed
- When management module redundancy is disabled, unless there is a hardware failure and the system is rebooted.

When a management module crashes while the other management module is rebooting

If the uncommon situation occurs where the active management module (MM1) is trying to reboot and the standby management module (MM2) also crashes, the switch attempts to recover from the crash and eventually the standby management module becomes the active management module if it passes self-test. However, traffic can be disrupted for as long as five minutes before the newly active management module (MM2) has finished rebooting.

About hotswapping out the active management module

You can hotswap out the active management module and have switch operations taken over by the standby management module by following the correct shutdown procedure on the active module using the **MM Shutdown** button. When the **MM Shutdown** button is pressed, any file synchronization in progress completes before the shutdown begins, and then a graceful shutdown of that management module occurs.

For information on using the **MM Shutdown** button, see “Hotswapping out the active management module” (page 250).

When the standby module is not available

If you have disabled management module redundancy with the `no redundancy management-module` command, or the standby module failed selftest, the **Dwn** LED does not turn green to indicate it is OK to hotswap out the active management module.

NOTE: If you remove the active management module without pressing the **MM Shutdown** button, any files that may have been in the process of synchronizing will not finish synchronizing to the standby module and all file transfer is aborted.

Hotswapping in a management module

If another management module is hotswapped in while there is an active management module booted up, the newly hotswapped management module becomes the standby module.

No negotiating is needed as to which module becomes the active management module, because there is already a functioning active management module. However, the following conditions must be met to determine if the hotswapped module can become a standby management module:

- The hotswapped module must pass selftest
- Management module redundancy is not administratively disabled (using the `no redundancy management-module` command). If the active management module's config file has redundancy administratively disabled, the hotswapped management module goes into "offline" mode.

In nonstop switching mode—The active management module's files and features are synced with the standby management module. Heartbeats are sent back and forth, and the standby management module is ready to quickly take over in the event of a switchover or a failure on the active management module.

In warm-standby mode—The standby management module partially boots up and heartbeats are sent back and forth with the active management module.

Software version mismatch between active and hotswapped module

If the software version in the hotswapped module does not match the software version in the active module, the following occurs:

1. The active module sends the primary and secondary images in flash to the hotswapped module.
2. The module that was hotswapped in then reboots if necessary to primary or secondary flash, whichever matches (if it does not already match).
3. After the hotswapped management module finishes booting, it is sent the config and other critical files from the active management module.
4. The hotswapped management module goes into standby mode and is ready to take over in case of a switchover.

NOTE: After the `boot standby` command is executed, if the software versions on the active management module and the standby management module are not compatible, the standby module does not sync with the active management module. The standby module then enters warm-standby redundancy mode.

Other software version mismatch conditions

The following steps describe the behavior that may when a new software image is installed in secondary flash of the AMM and a `redundancy switchover` command is executed.

1. A new software image, K.15.04.0002 containing ROM upgrade K.15.12 is installed in secondary flash of the AMM/MM1.
2. The AMM/MM1 automatically syncs the images to the secondary flash in the SMM/MM2. Now both AMM/MM1 and SMM/MM2 have identical software and ROM in secondary flash.
3. The SMM/MM2 is booted from secondary. It boots into the new K.15.04.0002 software version. The new ROM is applied and the SMM/ MM2 reboots.
4. After the SMM/MM2 finishes rebooting, it reconnects to the AMM/MM1 and prepares to take the standby role by rebooting.
5. However, the AMM/MM1 is running software version K.15.03.0008 in its primary flash, and the SMM/MM2 is running software version K.15.04.0002 in its secondary flash, so the SMM/MM2 pauses its reboot because of the software mismatch.
6. If a `redundancy switchover` command is executed, the AMM/MM1 will give control to the SMM/MM2, which can then finish booting and become the new AMM/MM2. This is the warm-start behavior.

7. The SMM/MM1 (former AMM/MM1) reboots, but unless the reboot is executed from secondary flash, it reboots into primary flash, which contains the older software version K.15.03.0008 with no ROM upgrade.
8. If the SMM/MM1 is forced to boot from secondary before executing the `redundancy switchover` command, it will boot into the new K.15.04.0002 software and upgrade the ROM. After the reboot that occurs with the ROM upgrade, the SMM/MM1 connects to the new AMM/MM2 and takes the standby role.

About downloading a new software version

File synchronization after downloading

After downloading a new software version to either the primary or secondary flash of the active management module, the software version is immediately copied to the corresponding flash (primary or secondary) of the standby module, unless the standby module failed selftest or redundancy was disabled with the `no redundancy management-module` command.

The configuration files, including which configuration file to use for that flash image, are synchronized. For example, if the active management module is using `config1`, the standby module is also synchronized to use `config1`.

Table 28 Example of upgrading software version K.15.01.0003 to version K.15.01.0004

	Newer code to secondary flash		New code to primary flash	
	Active MM	Standby MM	Active MM	Standby MM
Software version downloaded to Primary flash image	K.15.01.0003	K.15.01.0003	K.15.01.0004	K.15.01.0004
Software version downloaded to Secondary flash image	K.15.01.0004	K.15.01.0004	K.15.01.0003	K.15.01.0003

NOTE: For information about testing new software versions, see "Setting the default flash for boot (CLI)" (page 256).

After installing the new software to the active management module, wait a few minutes, and then verify that the standby management module has been synchronized with the new software as well (use the `show flash` command). If the default flash for boot is set correctly, you can start the standby management module on the new software by executing the `boot standby` command. This does not interrupt current switch operations yet. After the standby management module has rebooted and is ready for takeover in standby mode (you can verify this using the `show redundancy` command—see syntax (page 242)), you can now switch over to the management module running the newer software with this command:

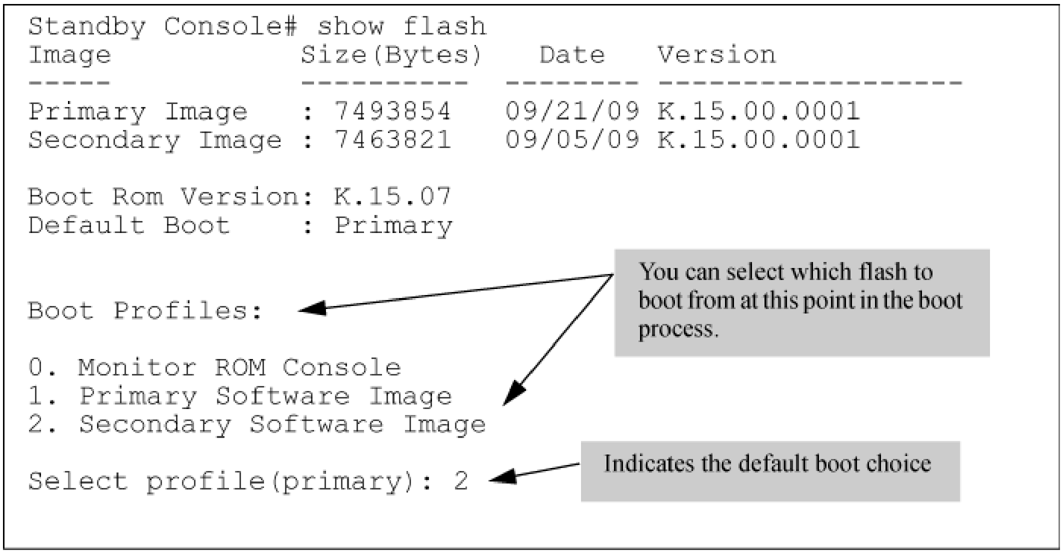
```
HP Switch# redundancy switchover
```

This causes a switchover to the management module that received the new software version, which becomes the active management module. This method incurs the least amount of network downtime for booting. If downtime is not an issue, use the `boot system` command. Both management modules are then running the new software version.

Potential software version mismatches after downloading

When a new software version is downloaded to the active management module, it is immediately copied to the corresponding flash (primary or secondary) in the standby management module, unless redundancy has been disabled. If the standby management module is rebooted, it will be running a different software version than the active management module. You can direct the standby module to boot from the non-corresponding flash image that has a different software version during the actual reboot process of the standby module when the prompt to select the **Boot Profile** appears, as shown in Figure 134 (page 272).

Figure 134 Booting the standby management module to secondary flash



```
Standby Console# show flash
Image              Size(Bytes)   Date     Version
-----              -----------  --------- ------------------
Primary Image    : 7493854      09/21/09 K.15.00.0001
Secondary Image  : 7463821      09/05/09 K.15.00.0001

Boot Rom Version: K.15.07
Default Boot    : Primary


Boot Profiles:

0. Monitor ROM Console
1. Primary Software Image
2. Secondary Software Image

Select profile(primary): 2
```

You can select which flash to boot from at this point in the boot process.

Indicates the default boot choice

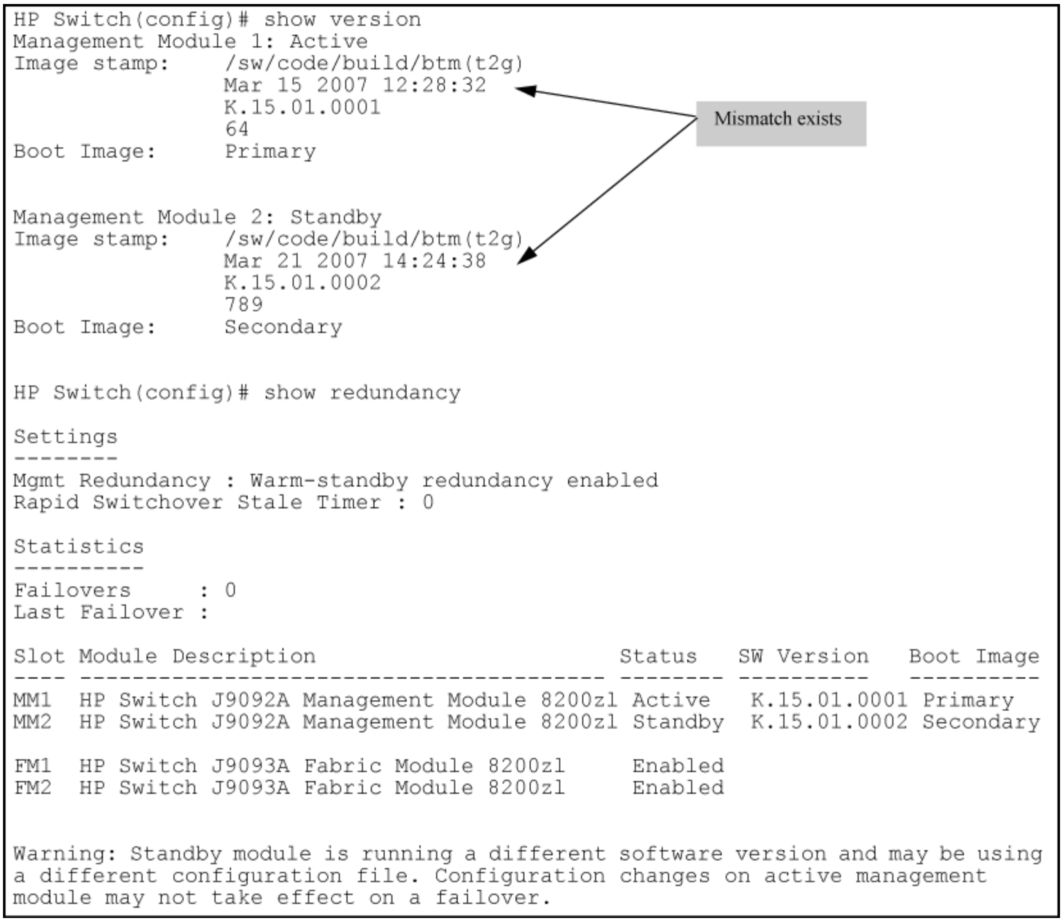
CAUTION: If you have booted one module out of primary flash and one module out of secondary flash, and the secondary flash is running a prior software version because the latest version was never copied over from the primary flash, you will have a software version mismatch. The configuration file may not work with that software version. For more information, see "Software version mismatch between active and hotswapped module" (page 270).

The standby module enters warm-standby redundancy mode and boots to a certain point, syncs basic files such as the config and security files, and finishes booting only if the active management module fails or you choose to change which module is the active module..

Additionally, if a switchover occurs, or if you reboot to make the standby module become the active module, any configuration file changes made may not work on the active module if it has a different software version from the standby module.

When you enter the `show redundancy` command and a software version mismatch exists, a warning message is displayed, as shown at the bottom of Figure 135 (page 273).

Figure 135 Example of a software version mismatch between the active and standby modules



```
HP Switch(config)# show version
Management Module 1: Active
Image stamp:    /sw/code/build/btm(t2g)
                Mar 15 2007 12:28:32
                K.15.01.0001
                64
Boot Image:     Primary


Management Module 2: Standby
Image stamp:    /sw/code/build/btm(t2g)
                Mar 21 2007 14:24:38
                K.15.01.0002
                789
Boot Image:     Secondary


HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Warm-standby redundancy enabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                        Status   SW Version   Boot Image
---- ---------------------------------------- -------- ----------   ----------
MM1  HP Switch J9092A Management Module 8200zl Active   K.15.01.0001 Primary
MM2  HP Switch J9092A Management Module 8200zl Standby  K.15.01.0002 Secondary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Enabled


Warning: Standby module is running a different software version and may be using
a different configuration file. Configuration changes on active management
module may not take effect on a failover.
```

Downloading a software version serially if the management module is corrupted

If the software version on a management module becomes corrupted, you may need to do a serial download to restore the affected module. The non-corrupted management module becomes the active module. You can then use the serial port on the corrupted management module to download a new software version. When the corrupted module is rebooted, the software version in the corrupted module is immediately overwritten by the software version in the active management module. Both management modules should now operate on the same software version.

About turning off redundant management

Disable management module redundancy with two modules present

To troubleshoot a suspect management module, you may want to operate the switch with redundant management disabled by entering this command:

```
HP Switch(config)# no redundancy management-module
```

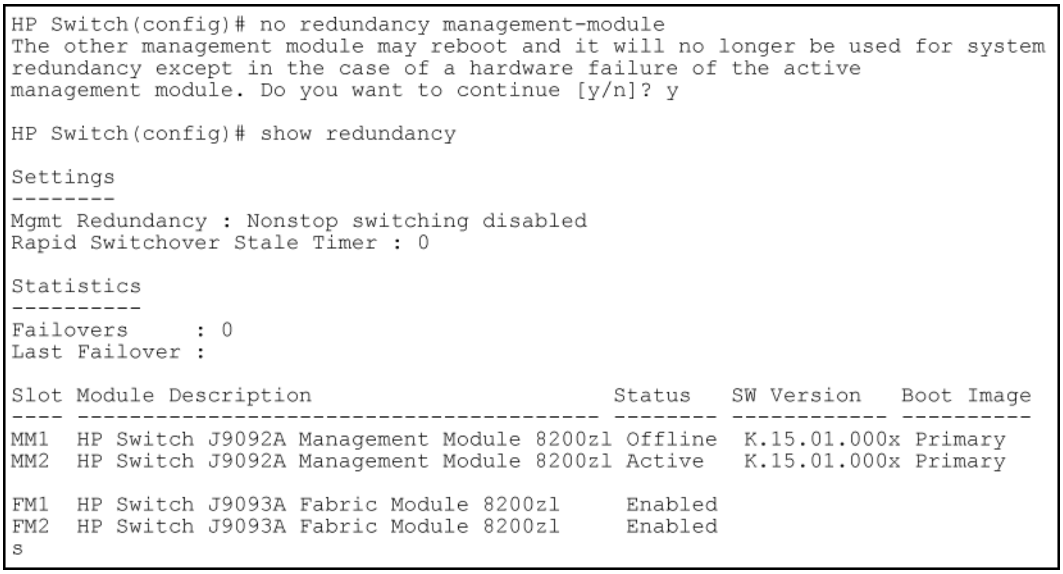
After executing this command, the second management module will not boot into standby mode—it is offline and no longer receives configuration file changes from the active module. The active management module updates its config file with the information that redundancy is disabled.

NOTE: Even if redundancy has been disabled, the specified management module becomes the active management module at the next system boot if you use the `redundancy active-management` command. You are warned that you may not be using current configurations. See "Setting the active management module for next boot (CLI)" (page 248).

The second management module is enabled as the active management module in the event of a hardware failure of the first management module.

Figure 136 (page 274) shows that redundant management was disabled.

Figure 136 Results of disabling redundancy



```
HP Switch(config)# no redundancy management-module
The other management module may reboot and it will no longer be used for system
redundancy except in the case of a hardware failure of the active
management module. Do you want to continue [y/n]? y

HP Switch(config)# show redundancy

Settings
--------
Mgmt Redundancy : Nonstop switching disabled
Rapid Switchover Stale Timer : 0

Statistics
----------
Failovers     : 0
Last Failover :

Slot Module Description                       Status   SW Version   Boot Image
---- ---------------------------------------- -------- ------------ ----------
MM1  HP Switch J9092A Management Module 8200zl Offline  K.15.01.000x Primary
MM2  HP Switch J9092A Management Module 8200zl Active   K.15.01.000x Primary

FM1  HP Switch J9093A Fabric Module 8200zl     Enabled
FM2  HP Switch J9093A Fabric Module 8200zl     Enabled
s
```

Disable management module redundancy with only one module present

If you disable redundancy when there is only one management module in the switch, and then you insert a second management module, the second module never goes into standby mode. You must re-enable redundant management using this command:

```
HP Switch(config)# redundancy management-module
```

The currently active module remains active on boot (assuming no selftest failure) unless you make the newly inserted management module active using this command:

```
HP Switch(config)# redundancy active-management standby
```

The standby management module becomes the active management module.

Active management module commands

Show modules

The `show modules` command displays information about all the modules in the switch, as well as additional component information for the following:

- System Support Modules (SSM)—identification, including serial number
- Mini-GBICS—a list of installed mini-GBICs displaying the type, "J" number, and serial number (when available)

CLI commands affected by redundant management

Several existing commands have changes related to redundant management.

boot command

In redundant management systems, the boot or boot active command causes a switchover to the standby management module as long as the standby module is in standby mode. This message displays:

```
This management module will now reboot and will become the
standby module! You will need to use the other management
module's console interface. Do you want to continue [y/n]?
```

If you select **y**, switchover is initiated by the standby management module, which becomes the active management module after boot completes.

If the standby module is not in standby mode (for example, it is in failed mode or offline mode), switchover to the standby module does not occur. The system is rebooted and this message displays:

```
The other management module is not in standby mode and this
command will not cause a switchover, but will reboot the
system, do you want to continue [y/n]?
```

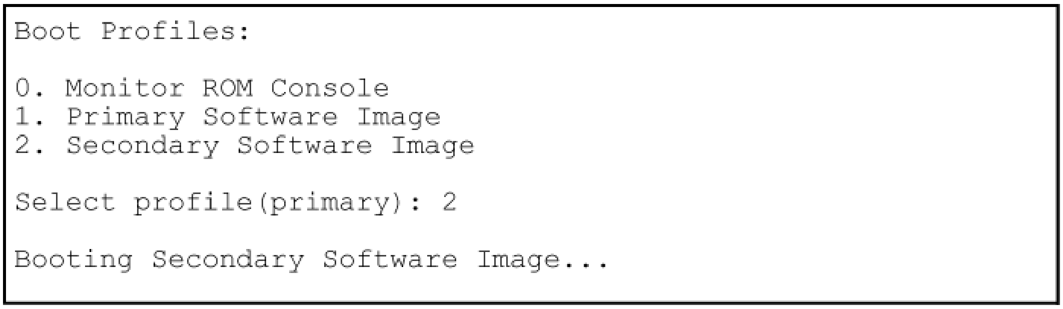
If the other management module is not present in the switch, the system simply reboots.

The boot command has these options.

Command	Action
boot cr	Reboots the active management module from the flash image that is specified for the default boot. This can be changed with the boot set-default flash command. You can select which image to boot from during the boot process itself. (See Figure 137 (page 276).) The switch will switchover to the standby management module. **NOTE:** This is changed from always booting from primary flash. You are prompted with a message, which indicates the flash being booted from.
boot active	Boots the active management module. The switch starts to boot from the default flash image. You can select which image to boot from during the boot process itself. (See Figure 137 (page 276).) The switch will switchover to the standby management module. If a second management module is not present in the switch, the system is rebooted.
boot standby	Boots the standby management module. The switch does not switchover. If the standby module is not present, this message displays: "The other management module is not present."
boot system[flash [primary | secondary]]	Boots both the active and standby management modules. You can specify the flash image to boot from.
boot set-default flash primary | secondary	Sets the default flash for the next boot to primary or secondary. You see this message: "This command changes the location of the default boot. This command will change the default flash image to boot from flash chosen>. Hereafter, 'reload' and 'boot' commands will boot from flash chosen>. Do you want to continue [y/n]?"

You can select a **boot profile** during the reboot process, as shown in Figure 137 (page 276). If you make no selection, the boot defaults to the image displayed as the default choice (shown in parentheses).

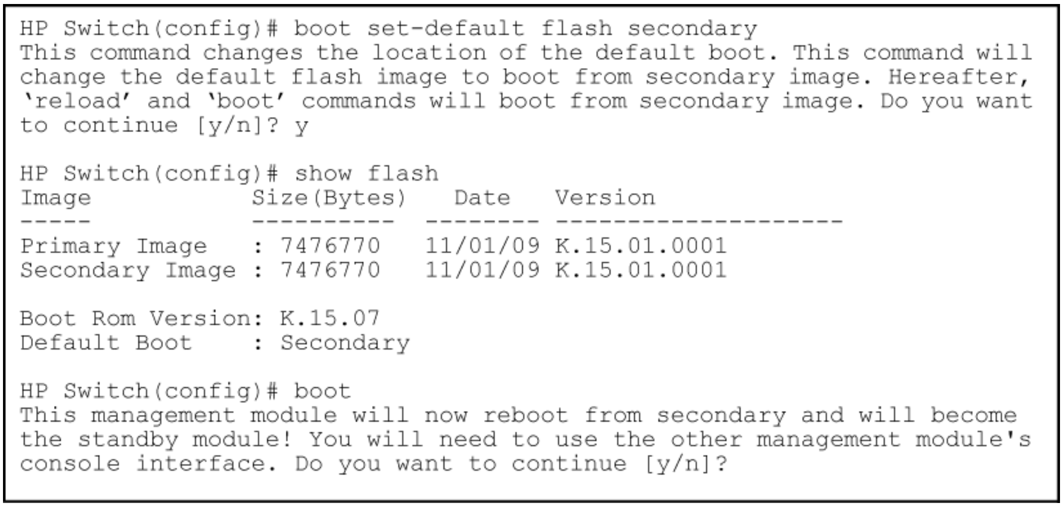
Figure 137 The management module rebooting, showing boot profiles to select



```
Boot Profiles:

0. Monitor ROM Console
1. Primary Software Image
2. Secondary Software Image

Select profile(primary): 2

Booting Secondary Software Image...
```

An example of the `boot` command with the **default flash** set to **secondary** is shown in Figure 138 (page 276).

Figure 138 Showing boot command with default flash set to secondary



```
HP Switch(config)# boot set-default flash secondary
This command changes the location of the default boot. This command will
change the default flash image to boot from secondary image. Hereafter,
'reload' and 'boot' commands will boot from secondary image. Do you want
to continue [y/n]? y

HP Switch(config)# show flash
Image              Size(Bytes)   Date     Version
-----              ----------  --------- --------------------
Primary Image    : 7476770     11/01/09 K.15.01.0001
Secondary Image  : 7476770     11/01/09 K.15.01.0001

Boot Rom Version: K.15.07
Default Boot     : Secondary

HP Switch(config)# boot
This management module will now reboot from secondary and will become
the standby module! You will need to use the other management module's
console interface. Do you want to continue [y/n]?
```

△ **CAUTION:** For a given reboot, the switch automatically reboots from the `startup-config` file assigned to the flash (primary or secondary) being used for the current reboot. The `startup-default` command can be used to set a boot configuration policy. This means that both the flash image and one of the three configuration files can be specified as the default boot policy. For more information on multiple configuration files and how they are used, see *"Multiple Configuration Files"* in the *"Switch Memory and Configuration"* chapter in this guide.

Boot and `reload` commands with OSPFv2 or OSPFv3 enabled

It is now possible to gracefully shut down OSPFv2 or OSPFv3 routing on HP switches without losing packets that are in transit. OSPF neighbors are informed that the router should not be used for forwarding traffic, which allows for maintenance on the switch without interrupting traffic in the network. There is no effect on the saved switch configuration

Prior to a switch shutdown, the CLI/SNMP `reload` command or the CLI `boot` command is executed to initiate the sending of OSPF "empty Hello list" messages on the interfaces that are part of the OSPF routing configuration. After a small delay (approximately 2 seconds) that allows the messages to be transmitted on all applicable interfaces the `boot` or `reload` command continues.

Modules operating in nonstop mode

When a switch is in standalone mode and OSPF routing is enabled, the "empty Hello list" is transmitted whenever the `boot` or `reload` command is executed.

When the switch is operating in nonstop switching mode (redundant), and a single module is being reloaded or booted, the standby module notifies neighboring switches of the management module failover. If the failover fails, the "empty Hello list" is transmitted before the switch is rebooted.

When a switch is operating with multiple management modules in warm standby mode, the "empty Hello list" is sent when a `reload` or `boot` command is executed. The standby management module sends out OSPF Hello packets after becoming the active management module.

Additional commands affected by redundant management

The other existing commands operate with redundant management as shown below.

Command	Action
`auto-tftp`	If a new image is downloaded using `auto-tftp`, the active management module downloads the new software version to both the active and standby modules. Rebooting after the `auto-tftp` completes reboots the entire system.
`banner`	The banner will not been seen on the standby module, only the active module.
`chassislocate`	If the management module performs a switchover, the LED does not remain lit.
`clear`	The `clear crypto` command causes public keys to be deleted from both modules when the second module is in standby mode.
`console`	Console settings, such as mode, flow-control, and baud-rate, are the same on both management modules. There cannot be individual settings for each management module.
`copy`	Files are automatically sync'd from the active management module to the standby management module. When no parameter is specified with the `copy crash-data` or `copy crash-log` command, files from all modules (management and interface) are concatenated. See "Copying crash file information to another file (CLI)" (page 259). **NOTE:** If redundancy is disabled or the standby module failed selftest, the `copy` command affects only the active management module.
`copy core-dump [ mm | standby | flash | xmodem | usb` *`filename`* `]`	The `copy core-dump standby flash` command copies the standby management module's coredump to the active management module's flash. The destination file is fixed as dumpM1.cor or dumpM2.cor, depending on which module is the standby management module. The `copy core-dump [ mm | standby | flash | xmodem | usb` *`filename`* `]` command copies the core file of the active management module or the standby management module to a USB flash drive or to an xmodem host.
`core-dump management-module`	Enables or disables a core dump on a management module.
`crypto`	Authentication files for ssh or the https server are copied to the standby management module. The `clear crypto` command deletes the public keys from both modules when the second module is in standby mode.
`erase flash`	Erases the software version on the active and standby modules. If redundancy has been disabled, or if the standby module has not passed selftest, the flash is not erased on the standby module.
`erase config`	Erases the config file on the active and standby modules. If redundancy has been disabled, or if the standby module has not passed selftest, the config file is not erased on the standby module.

Command	Action
`erase startup-config`	Affects both modules if the second module is in standby mode. If redundancy has been disabled, or if the standby module has not passed selftest, the `startup-config` file is not erased on the standby module.
`fastboot`	When fastboot is enabled, this information is saved to the standby management module when the config files are sync'd. The fastboot value is used during the next boot on both modules.

`front-panel-security`
`factory-reset`
`password-clear`
`password-recovery`
	This command and its options affect only the active management module. See the section "Front-Panel Button Functions" in the *Access Security Guide* for more information about resetting the switch.

`kill`	Does not affect the console on the standby module.
`log`	Log messages from a formerly active management module are available on the current active management module after a switchover.
`password (set` or `clear)`	Affects only the active management module until a switchover occurs, at which time it affects the new active module.
`startup-default`	Affects both modules. The config file is immediately sent to the standby module and also becomes the default on that module when the next boot occurs.
`update`	Affects only the active module. The standby may become the active module when the updated active module is booted.
`write`	A `write memory` updates the config file in flash on the active module. The file is then sync'd to the standby module.

Using the WebAgent for redundant management

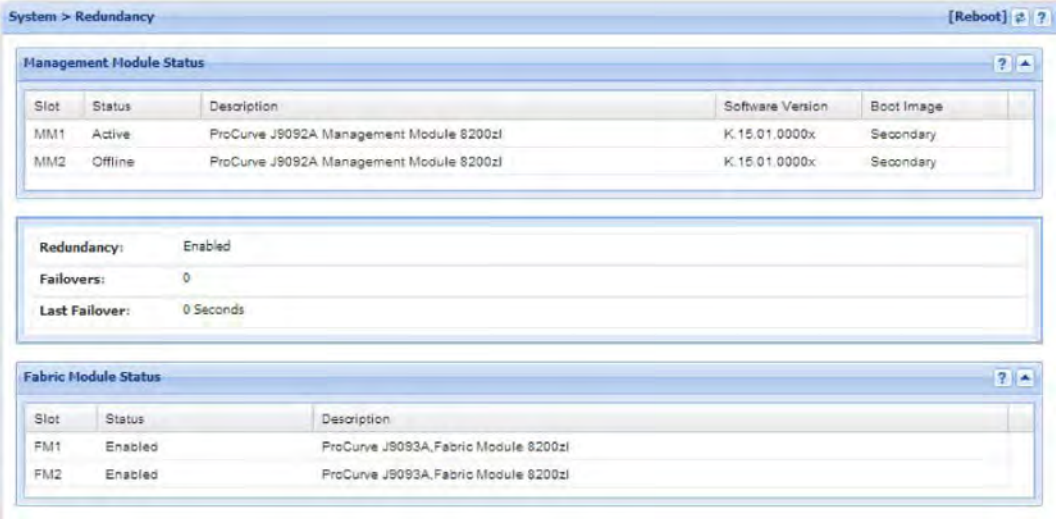
The WebAgent can be used to display information about the active and standby management modules.

Online Help is available for the WebAgent, which you can open by clicking on the question mark (?) in the upper right corner of any of the WebAgent screens. An example redundancy screen is shown in Figure 139 (page 279).

To access the redundancy information in the WebAgent:

1. In the WebAgent navigation panel, click System.
2. Click Redundancy. The following screen displays.

Figure 139 Example of redundancy screen in the WebAgent



System > Redundancy [Reboot]

Management Module Status

Slot	Status	Description	Software Version	Boot Image
MM1	Active	ProCurve J9092A Management Module 8200zl	K.15.01.0000x	Secondary
MM2	Offline	ProCurve J9092A Management Module 8200zl	K.15.01.0000x	Secondary

Redundancy:	Enabled
Failovers:	0
Last Failover:	0 Seconds

Fabric Module Status

Slot	Status	Description
FM1	Enabled	ProCurve J9093A,Fabric Module 8200zl
FM2	Enabled	ProCurve J9093A,Fabric Module 8200zl

Notes on how the active module is determined

Both management modules run selftest routines to determine which module becomes the active management module and which becomes the standby management module. The module that was last active in the chassis is given precedence and becomes the "active" module. This module is the one that is booted going forward. If a module fails selftest and is unable to communicate with the other module, it does not take control as the management module. The other management module takes control and becomes the active module.

If both modules fail selftest, the fault LED flashes and neither module is operational.

NOTE: You are not allowed to switchover to a management module that is not in standby mode. The module must have passed selftest and be in standby mode.

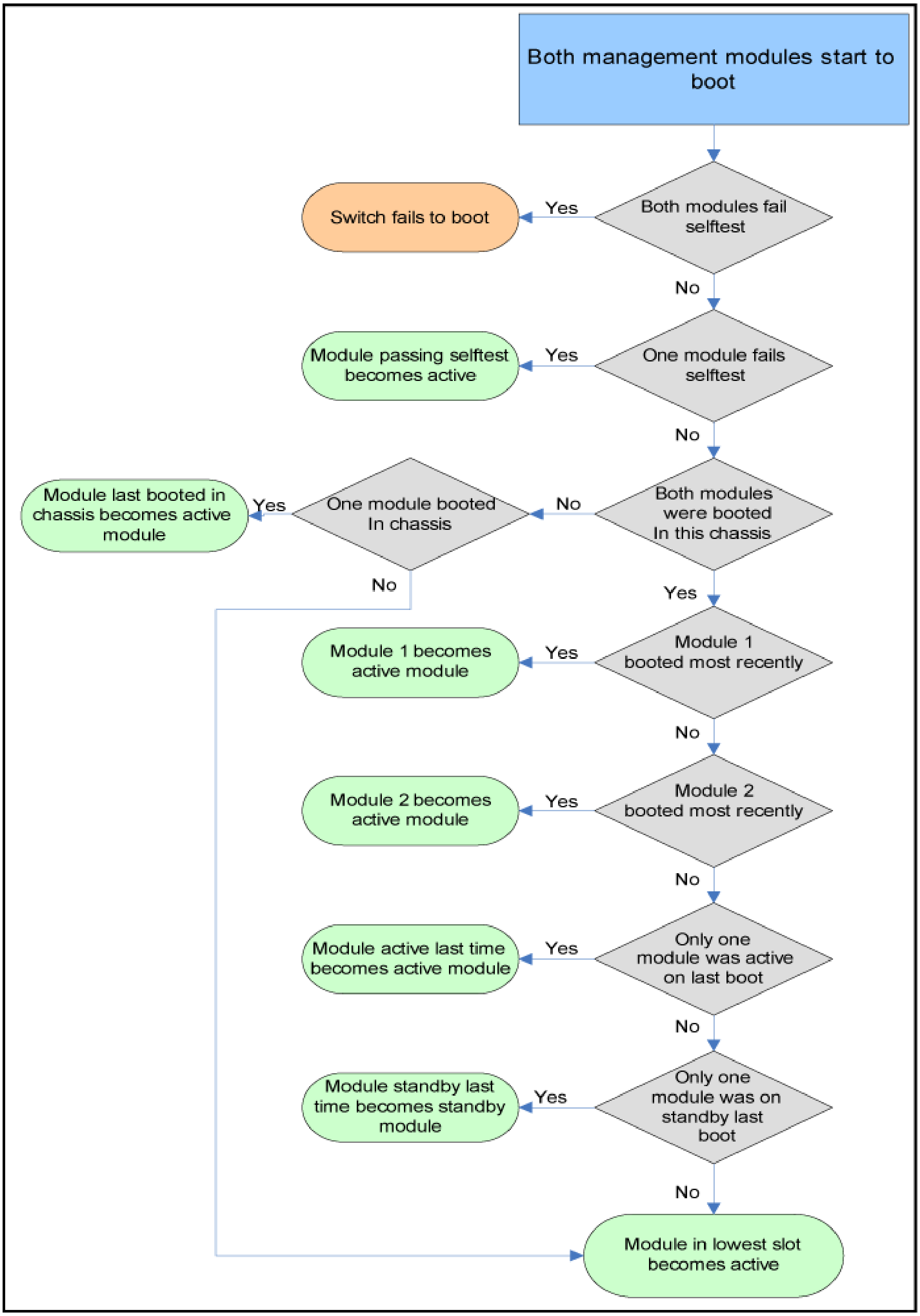
The entire boot decision process works as follows:

1. If there is only one management module, that is the active management module.
2. If one module is already booted and operational, a newly inserted module or the other management module booting always becomes the standby module. The standby module does not become active unless a switchover occurs.
3. If there are two management modules and one fails selftest, the one that passes selftest becomes the active management module.
4. If only one of two modules was ever booted in the chassis, that module is given precedence.
5. The module that was active on the last boot becomes the active management module. This guarantees that the active module has the latest configuration data.
6. If both management modules have previously booted in this chassis and were "active" the last time booted, the module that booted most recently becomes the active management module.
7. If none of the above conditions are applicable, the module in the lowest slot becomes the active management module.

To see a diagram of this process, see “Active module decision flow chart at boot” (page 280).

Diagram of the decision process

Figure 140 Active module decision flow chart at boot


Both management modules start to boot
Both modules fail selftest
Yes
Switch fails to boot
No
One module fails selftest
Yes
Module passing selftest becomes active
No
Both modules were booted In this chassis
No
One module booted In chassis
Yes
Module last booted in chassis becomes active module
No
Yes
Module 1 booted most recently
Yes
Module 1 becomes active module
No
Module 2 booted most recently
Yes
Module 2 becomes active module
No
Only one module was active on last boot
Yes
Module active last time becomes active module
No
Only one module was on standby last boot
Yes
Module standby last time becomes standby module
No
Module in lowest slot becomes active

CLI commands and syncing

The following CLI commands can be executed during initial syncing between the active management module and the standby management module, which occurs when the standby module is inserted or after a reboot of the system. All other CLI commands will not be executed until after the initial syncing completes.

During initial syncing, no SNMP set requests are executed, except the SNMP request for ping.

Operator commands		
`dir`	`menu`	`traceroute6`
`enable`	`ping`	`dbgstack`
`exit`	`ping6`	`wireless-services`
`link-test`	`show`	`services`
`logout`	`traceroute`	

Manager commands		
`boot system`	`copy running-config`	`page`
`boot active`	`copy startup-config`	`print`
`boot standby`	`copy event-log`	`redo`
`configure`	`copy core-dump`	`reload`
`copy command-output`	`recopy`	`repeat`
`copy config tftp`	`display`	`task-monitor`
`copy config xmodem`	`end`	`telnet`
`copy crash-data`	`getMIB`	`terminal`
`copy crash-log`	`kill`	`walkMIB`
`copy flash tftp`	`licenses`	`write-terminal`
`copy flash xmodem`	`log`	`redundancy`

Management module redundancy features

Nonstop switching features

Nonstop switching features are synced at initialization of the standby management module.

802.1X and Web/MAC authentication MAC Lockout/Lockdown ACLs/Qos Policies Power over Ethernet Port Security DHCP Snooping Dynamic ARP Protection Dynamic IP Lockdown	Spanning Tree (MSTP) GVRP Loop Protection LACP Syslog UDLD Virus Throttling LLDP

Unsupported zl modules

ZL modules/controllers that do not support the nonstop switching feature include the following:

- HP ONE Services zl Module (J9289A)
- HP Threat Management Services zl Module (J9155A)
- HP Threat Management Services zl Module with 1-year IDS/IPS subscription (J9156A)

- HP Wireless Edge Services zl Module (J9051A) and Redundant Wireless Services zl Module (J9052A)
- HP MSM765zl Mobility Controller (J9370A)

During a nonstop switching failover, unsupported modules will not failover seamlessly to the standby module. A nonstop switching failover causes a forced reboot on these modules. After rebooting, these modules then sync with the newly active management module and begin operation again. Module traffic is disconnected until the module completes the reboot process.

Hot swapping of management modules

Use the MM Shutdown button on the front of the management module before removal. The Shutdown button ensures that the management module is shut down properly. If nonstop switching is enabled, using the Shutdown button prior to removal ensures failover to the standby module will be successful.

Rapid routing switchover and stale timer

With K.15.01.0031, nonstop switching supports only Layer 2 functions on the switch. During a failover, traffic routed through the switch at Layer 3 will see an interruption. When a failover from active to standby occurs, the routing table is "frozen." All routes that existed at the time of the failover are marked as "stale." While dynamic routing protocols running at the time may act as if the routing protocol has been restarted and rebuilds the table, the switch on which the failover occurred continues to rout traffic using the ‘stale routes.'

The "stale timer" begins counting when the switchover occurs. When the "stale timer" expires, any routes that are still marked as stale are purged from the routing table. Because of the nature of rapid routing switchover, if there are multiple simultaneous failures, network loops could occur or traffic could flow through unpredictable paths.

Use caution if setting the "rapid-switchover" timer higher than the default. To disable "rapid routing switchover" and to ensure that all routing is based on the most current routing protocol information, set the "rapid-switchover" timer to 0.

A File transfers

Command summary

Table 29 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
copy tftp flash *ip-address remote-file* [primary | secondary] [oobm]	Automatically downloads a switch software file to primary or secondary flash.	Primary, unless specified	(page 286)	(page 288)
[no] tftp client | server [listen oobm | data | both]	Disables/re-enables TFTP for client or server functionality	-	(page 287)	-
auto-tftp *ip-addr filename*	Configures the switch to automatically download the specified software file from the TFTP server at the specified IP address.	Disabled	(page 287)	-
copy xmodem flash [primary | secondary]	Downloads a software file to primary or secondary flash.	Primary, unless specified	(page 290)	(page 291)
copy usb flash *filename* [primary | secondary]	Automatically downloads a switch software file to primary or secondary flash.	Primary, unless specified	(page 292)	-
copy tftp flash *ip-addr* flash [primary | secondary] [oobm]	Executed in the destination switch, downloads the software flash in the source switch's primary flash to either the primary or secondary flash in the destination switch.	Primary, unless specified	(page 293)	(page 294)
copy tftp flash *ip-addr* [/os/primary | /os/secondary] [primary | secondary] [oobm]	Executed in the destination switch, gives you the most options for downloading between switches.	-	(page 293)	-
copy flash tftp *ip-addr filename* [oobm]	Copies the primary flash image to a TFTP server.	-	(page 294)	-
copy flash xmodem [pc | unix]	Uses Xmodem to copy a designated configuration file from the switch to a PC or UNIX workstation.	-	(page 295)	-
copy flash usb *filename*	Uses the USB port to copy the primary flash image from the switch to a USB flash memory device.	-	(page 295)	-
copy [startup-config | running-config] tftp *ip-addr remote-file* [pc | unix] [oobm] copy config *filename* tftp *ip-addr remote-file* [pc | unix] [oobm]	Can copy a designated config file in the switch to a TFTP server.	-	(page 295)	-
copy tftp [startup-config | running-config *ip-addr remote-file*] [pc | unix] [oobm]	Can copy a configuration from a remote host to a designated config file in the switch.	-	(page 296)	-

Table 29 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`copy tftp config` *`filename`* *`ip-addr remote-file`* `[ pc | unix ]` [oobm]				
`copy tftp show-tech ipv4 or ipv6 address` *`filename`* [oobm]	Copies a customized command file to the switch.	-	(page 296)	-
`show tech custom`	Executes the commands found in a custom file instead of the hard-coded list.	-	(page 297)	-

`copy` [[`startup-config] | running-config`] `xmodem` [`pc | unix ]`
`copy config` *`filename`* `xmodem [ pc | unix ]`
	Uses Xmodem to copy a designated configuration file from the switch to a PC or UNIX workstation.	-	(page 297)	-

`copy xmodem startup-config` [`pc | unix ]`
`copy xmodem config` *`filename`* `[ pc | unix ]`
	Copies a configuration file from a serially connected PC or UNIX workstation to a designated configuration file on the switch.	-	(page 298)	-

`copy startup-config usb` *`filename`*
`copy running-config usb` *`filename`*
	Uses the USB port to copy a designated configuration file from the switch to a USB flash memory device.	-	(page 298)	-

`copy usb startup-config` *`filename`*	Copies a configuration file from a USB device to the startup configuration file on the switch.	-	(page 299)	-
`copy tftp command-file` *`ip-addr filename`*`.txt [ unix | pc`] [oobm]	Copies and executes the named text file from the specified TFTP server address and executes the ACL commands in the file.	-	(page 299)	-
`copy xmodem command-file unix | pc`	Uses Xmodem to copy and execute an ACL command from a PC or UNIX workstation.	-	(page 300)	-
`copy usb command-file` *`filename`*`.txt [ unix | pc ]`	Copies and executes the named text file from a USB flash drive and executes the ACL commands in the file.	-	(page 301)	-

`copy command-output "`*`cli-command`*`" tftp` *`ip-address filepath-filename`* [oobm]
`copy command-output "`*`cli-command`*`" usb` *`filename`*
`copy command-output "`*`cli-command`*`" xmodem`
	Direct the displayed output of a CLI command to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.	-	(page 301)	-

`copy event-log smm tftp | usb | xmodem`
`copy event-log tftp` *`ip-address filepath_filename`* [oobm]
`copy event-log usb` *`filename`*
	Copy the Event Log content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.	-	(page 302)	-

Table 29 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`copy event-log xmodem` *`filename`*				

`copy crash-data [ ` *`slot-id`* ` | master ]`
`tftp ` *`ip-address filename`* `[oobm]`
`copy crash-data [ ` *`slot-id`* ` | mm ]`
`usb ` *`filename`*
`copy crash-data [ ` *`slot-id`* ` | mm ]`
`xmodem`
	Copy the crash data content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.	-	(page 302)	-

`copy crash-data [ ` *`slot-id`* ` | mm ] tftp ` *`ip-address filename`* `[oobm]`	Copies the crash data of both the active and standby management modules to a user-specified file.	-	(page 303)	-

`copy crash-log [ ` *`slot-id`* ` | mm ] tftp ` *`ip-address filepath and filename`* ` [oobm]`
`copy crash-log [ ` *`slot-id`* ` | mm ] usb ` *`filename`*
`copy crash-log [ ` *`slot-id`* ` | mm ] xmodem`
	Copy the Crash Log content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.	-	(page 303)	-

`copy crash-log [ ` *`slot-id`* ` | mm ] tftp ` *`ip-address filepath and filename`* ` [oobm]`	Copies the crash logs of both the active and standby management modules to a user-specified file.	-	(page 304)	-
`copy core-dump [ mm usb ` *`filename`* ` | standby flash | usb ` *`filename`* ` ]`	Copies the management module coredump or the standby management module coredump to the active management module flash or to a USB flash drive.	-	(page 305)	-

`usb-port`
`no usb-port`
	Enables the USB port.	-	(page 305)	-

`show usb-port`	Displays the status of the USB port.	-	(page 306)	-
`[no] autorun [ encryption-key ` *`key-string`* ` | secure-mode ]`	Enables/disables USB autorun on the switch.	Enabled	(page 307)	-

Overview

The switches support several methods for transferring files to and from a physically connected device or via the network, including TFTP, Xmodem, and USB. This appendix explains how to download new switch software, upload or download switch configuration files and software images, and upload command files for configuring ACLs.

For general information about downloading software, see the section starting with "About downloading switch software" (page 308).

Using TFTP to download software from a server

This procedure assumes that:

- A software version for the switch has been stored on a TFTP server accessible to the switch. (The software file is typically available from the HP Switch Networking website at **www.procurve.com**.)
- The switch is properly connected to your network and has already been configured with a compatible IP address and subnet mask.
- The TFTP server is accessible to the switch via IP.

Before you use the procedure, do the following:

- Obtain the IP address of the TFTP server in which the software file has been stored.
- If VLANs are configured on the switch, determine the name of the VLAN in which the TFTP server is operating.
- Determine the name of the software file stored in the TFTP server for the switch (for example, E0820.swi).

NOTE: If your TFTP server is a UNIX workstation, ensure that the case (upper or lower) that you specify for the filename is the same case as the characters in the software filenames on the server.

Downloading from a server to flash using TFTP (CLI)

Syntax:

`copy tftp flash` *`ip-address remote-file`* `[ primary | secondary ][oobm]`

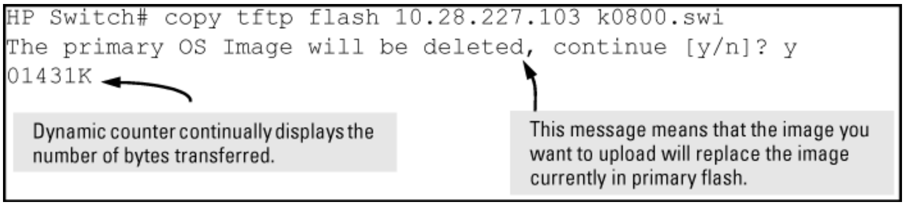
Automatically downloads a switch software file to primary or secondary flash. If you do not specify the flash destination, the TFTP download defaults to primary flash.

Example

To download a switch software file named k0800.swi from a TFTP server with the IP address of 10.28.227.103 to primary flash:

1. Execute `copy` as shown below:

Figure 141 Example of the command to download an OS (switch software)



```
HP Switch# copy tftp flash 10.28.227.103 k0800.swi
The primary OS Image will be deleted, continue [y/n]? y
01431K
```

Dynamic counter continually displays the number of bytes transferred.

This message means that the image you want to upload will replace the image currently in primary flash.

When the switch finishes downloading the software file from the server, it displays this progress message:

Validating and Writing System Software to FLASH ...

2. When the download finishes, you must reboot the switch to implement the newly downloaded software image. To do so, use one of the following commands:

Syntax:

```
boot system flash[ primary | secondary ]
```

Boots from the selected flash.

Syntax:

```
reload
```

Boots from the flash image and startup-config file. A switch covered in this guide (with multiple configuration files), also uses the current startup-config file.

For more information on these commands, see "Rebooting the Switch" in the *Basic Operation Guide* for your switch.

3. To confirm that the software downloaded correctly, execute `show system` and check the **Firmware revision** line.

For information on primary and secondary flash memory and the boot commands, see "Using Primary and Secondary Flash Image Options" in the *Basic Operation Guide* for your switch.

NOTE: If you use `auto-tftp` to download a new image in a redundant management system, the active management module downloads the new image to both the active and standby modules. Rebooting after the `auto-tftp` process completes reboots the entire system.

Enabling TFTP (CLI)

TFTP is enabled by default on the switch. If TFTP operation has been disabled, you can re-enable it by specifying TFTP client or server functionality with the

```
tftp[ client | server ]
```

command at the global configuration level.

Syntax:

```
[ no ] tftp[ client | server [ listen oobm | data | both ]  ]
```

Disables/re-enables TFTP for client or server functionality so that the switch can:

- Use TFTP client functionality to access TFTP servers in the network to receive downloaded files.
- Use TFTP server functionality to upload files to other devices on the network.

For switches that have a separate out-of-band management port, the `listen` parameter in a **server** configuration allows you to specify whether transfers take place through the out-of-band management (oobm) interface, the data interface, or both. For more information on OOBM, see “Network Out-of-Band Management (OOBM) for the 6600 Switch” (page 492).

Usage notes:

To disable all TFTP client or server operation on the switch except for the auto-TFTP feature, enter the `no tftp [client|server]` command.

When IP SSH file transfer is used to enable SCP and SFTP functionality on the switch, this disables TFTP client and server functionality. Once ip ssh file transfer is enabled, TFTP and auto-TFTP cannot be re-enabled from the CLI.

When TFTP is disabled, instances of TFTP in the CLI `copy` command and the Menu interface "Download OS" screen become unavailable.

The `no tftp <client | server>` command does not disable auto-TFTP operation. To disable an auto-TFTP command configured on the switch, use the `no auto-tftp` command described on page “Configuring the switch to download software automatically from a TFTP server using auto-TFTP (CLI)” (page 287) to remove the command entry from the switch's configuration.

For information on how to configure TFTP file transfers on an IPv6 network, see the "IPv6 Management Features" chapter in the *IPv6 Configuration Guide* for your switch.

Configuring the switch to download software automatically from a TFTP server using auto-TFTP (CLI)

The `auto-tftp` command lets you configure the switch to download software automatically from a TFTP server.

At switch startup, the auto-TFTP feature automatically downloads a specified software image to the switch from a specified TFTP server and then reboots the switch. To implement the process, you must first reboot the switch using one of the following methods:

- Enter the `boot system flash primary` command in the CLI.
- With the default flash boot image set to primary flash (the default), enter the `boot` or the `reload` command, or cycle the power to the switch. (To reset the boot image to primary flash, use `boot set-default flash primary`.)

Syntax:

`auto-tftp` *`ip-addr filename`*

By default, auto-TFTP is disabled. This command configures the switch to automatically download the specified software file from the TFTP server at the specified IP address. The file is downloaded into primary flash memory at switch startup; the switch then automatically reboots from primary flash.

NOTE: To enable auto-TFTP to copy a software image to primary flash memory, the version number of the downloaded software file (for example, K_14_01.swi) must be different from the version number currently in the primary flash image.

The current TFTP client status (enabled or disabled) does not affect auto-TFTP operation. (See “Enabling TFTP (CLI)” (page 287).)

Completion of the auto-TFTP process may require several minutes while the switch executes the TFTP transfer to primary flash and then reboots again.

The no form of the command disables auto-TFTP operation by deleting the `auto-tftp` entry from the startup configuration.

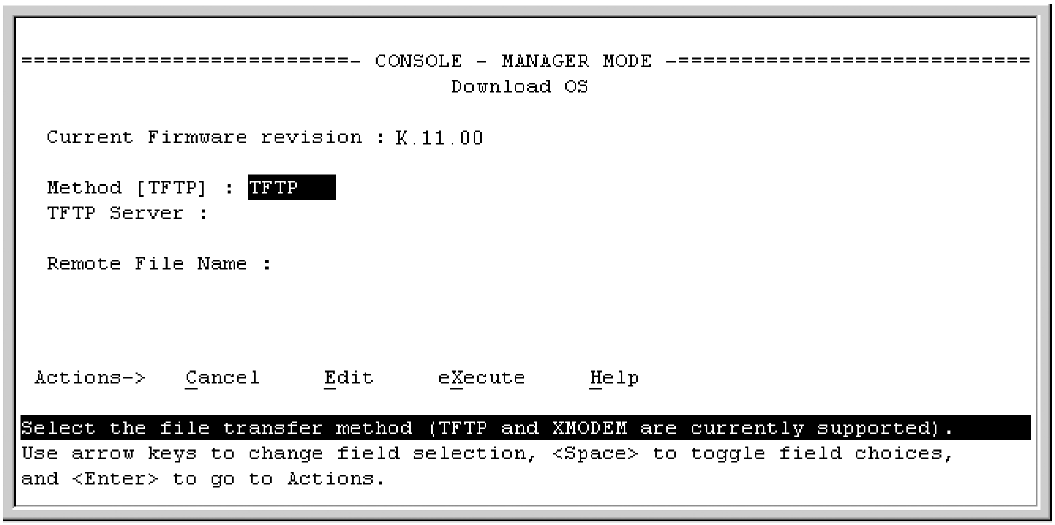
The `no auto-tftp` command does not affect the current TFTP-enabled configuration on the switch. However, entering the `ip ssh filetransfer` command automatically disables both `auto-tftp` and `tftp` operation.

Downloading from a server to primary flash using TFTP (Menu)

Note that the menu interface accesses only the primary flash.

1. In the console Main Menu, select **Download OS** to display the screen in Figure 142 (page 288). (The term "OS" or "operating system" refers to the switch software):

Figure 142 Example of a download OS (software) screen (default values)



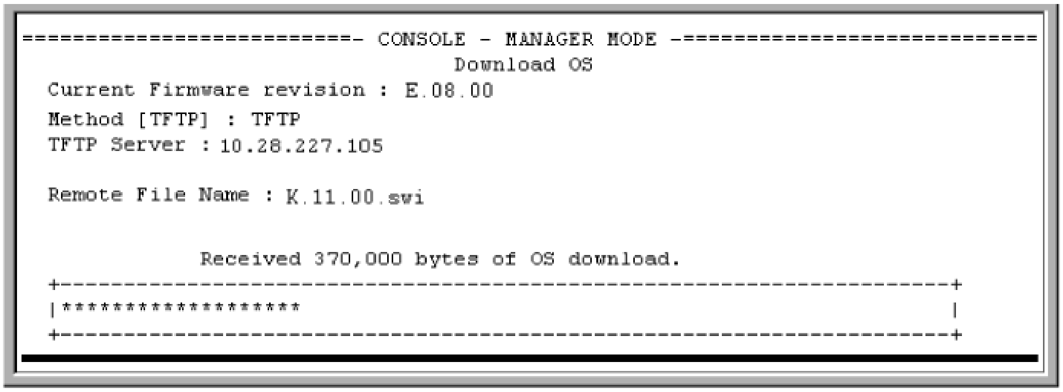
```
==========================- CONSOLE - MANAGER MODE -============================
                               Download OS

  Current Firmware revision : K.11.00

  Method [TFTP]  : TFTP
  TFTP Server :

  Remote File Name :



 Actions->   Cancel     Edit     eXecute     Help

Select the file transfer method (TFTP and XMODEM are currently supported).
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

2. Press **[E]** (for **Edit**).
3. Ensure that the **Method** field is set to **TFTP** (the default).

4. In the **TFTP Server** field, enter the IP address of the TFTP server in which the software file has been stored.
5. In the **Remote File Name** field, enter the name of the software file (if you are using a UNIX system, remember that the filename is case-sensitive).
6. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the software download.

   The screen shown in Figure 143 (page 289) appears:

   Figure 143 Example of the download OS (software) screen during a download

   ```
   =========================- CONSOLE - MANAGER MODE -===========================
                                  Download OS
     Current Firmware revision : E.08.00

     Method [TFTP] : TFTP
     TFTP Server : 10.28.227.105

     Remote File Name : K.11.00.swi


                Received 370,000 bytes of OS download.
     +-------------------------------------------------------------------------+
     |*******************                                                      |
     +-------------------------------------------------------------------------+
   ```

   A "progress" bar indicates the progress of the download. When the entire software file has been received, all activity on the switch halts and you will see **Validating and writing system software to FLASH...**
7. After the primary flash memory is updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**).

   You will see this prompt:

   ```
   Continue reboot of system? : No
   ```

   Press the space bar once to change **No** to **Yes**, then press **[Enter]** to begin the reboot.

   NOTE: When you use the menu interface to download a switch software, the new image is always stored in primary flash. Also, using the `Reboot Switch` command in the Main Menu always reboots the switch from primary flash. Rebooting the switch from the CLI provides more options. See "Rebooting the Switch" in the *Basic Operation Guide* for your switch.
8. After you reboot the switch, confirm that the software downloaded correctly:
   a. From the Main Menu, select
      2. Switch Configuration...
      2. Port/Trunk Settings

   b. Check the **Firmware revision** line.

For troubleshooting information on download failures, see "Troubleshooting TFTP download failures" (page 308).

Enabling SCP and SFTP

For more information about secure copy and SFTP, see "Using SCP and SFTP" (page 309).

1. Open an SSH session as you normally would to establish a secure encrypted tunnel between your computer and the switch.

   For more detailed directions on how to open an SSH session, see chapter "Configuring secure shell (SSH)" in the Access Security Guide for your switch. Please note that this is a one-time procedure for new switches or connections. If you have already done it once you should not need to do it a second time.

2. To enable secure file transfer on the switch (once you have an SSH session established between the switch and your computer), open a terminal window and enter the following command:

   ```
   HP Switch(config)# ip ssh filetransfer
   ```

For information on disabling TFTP and auto-TFTP, see "Disabling TFTP and auto-TFTP for enhanced security" (page 310).

Using Xmodem to download switch software from a PC or UNIX workstation

This procedure assumes that:

- The switch is connected via the Console RS-232 port to a PC operating as a terminal. (For information on connecting a PC as a terminal and running the switch console interface, see the *Installation and Getting Started Guide* you received with the switch.)
- The switch software is stored on a disk drive in the PC.
- The terminal emulator you are using includes the Xmodem binary transfer feature. (For example, in the HyperTerminal application included with Windows NT, you would use the **Send File** option in the **Transfer** drop-down menu.)

Downloading to primary or secondary flash using Xmodem and a terminal emulator (CLI)

Syntax:

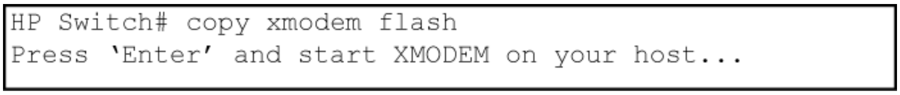
```
copy xmodem flash [  primary | secondary  ]
```

Downloads a software file to primary or secondary flash. If you do not specify the flash destination, the Xmodem download defaults to primary flash.

Example

To download a switch software file named `E0822.swi` from a PC (running a terminal emulator program such as HyperTerminal) to primary flash:

1. Execute the following command in the CLI:



```
HP Switch# copy xmodem flash
Press 'Enter' and start XMODEM on your host...
```

2. Execute the terminal emulator commands to begin the Xmodem transfer. For example, using HyperTerminal:
   a. Click on **Transfer**, then **Send File**.
   b. Type the file path and name in the Filename field.
   c. In the Protocol field, select **Xmodem**.
   d. Click on the **[Send]** button.

      The download can take several minutes, depending on the baud rate used in the transfer.
3. When the download finishes, you must reboot the switch to implement the newly downloaded software. To do so, use one of the following commands:

   ### Syntax:

   ```
   boot system flash [ primary | secondary ]
   ```

   Reboots from the selected flash

   ### Syntax:

   ```
   reload
   ```

   Reboots from the flash image currently in use

For more information on these commands, see “Rebooting the Switches”in the *Basic Operation Guide* for your switch.

4. To confirm that the software downloaded correctly:

   ```
   HP Switch show system
   ```

   Check the **Firmware revision** line. It should show the software version that you downloaded in the preceding steps.

If you need information on primary/secondary flash memory and the boot commands, see "Using Primary and Secondary Flash Image Options" in the *Basic Operation Guide* for your switch.

Downloading to primary flash using Xmodem (Menu)

NOTE: The menu interface accesses only the primary flash.

1. From the console Main Menu, select
   7. Download OS
2. Press **[E]** (for **Edit**).
3. Use the Space bar to select **XMODEM** in the **Method** field.
4. Press **[Enter]**, then **[X]** (for **eXecute**) to begin the software download.

   The following message appears:

   Press enter and then initiate Xmodem transfer from the attached computer.....
5. Press **[Enter]** and then execute the terminal emulator commands to begin Xmodem binary transfer.

   For example, using HyperTerminal:

   a. Click on **Transfer**, then **Send File**.
   b. Enter the file path and name in the Filename field.
   c. In the Protocol field, select **Xmodem**.
   d. Click on the **[Send]** button.

   The download then commences. It can take several minutes, depending on the baud rate set in the switch and in your terminal emulator.
6. After the primary flash memory has been updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**). You then see the following prompt:
   Continue reboot of system? : No

   Press the space bar once to change **No** to **Yes**, then press **[Enter]** to begin the reboot.
7. To confirm that the software downloaded correctly:

   a. From the Main Menu, select
      1. Status and Counters
      1. General System Information
   b. Check the **Firmware revision** line.

Downloading switch software using USB (CLI)

This procedure assumes that:

- A software version for the switch has been stored on a USB flash drive. (The latest software file is typically available from the HP Switch Networking website at **www.hp.com**.)
- The USB device has been plugged into the switch's USB port.

Before you use the procedure:

- Determine the name of the software file stored on the USB flash drive (for example, `k0800.swi`).
- Decide whether the image will be installed in the primary or secondary flash. For more on primary/secondary flash memory and related boot commands, see "Using Primary and Secondary Flash Image Options" in the *Basic Operation Guide* for your switch.

Syntax:

```
copy usb flash filename[  primary | secondary ]
```

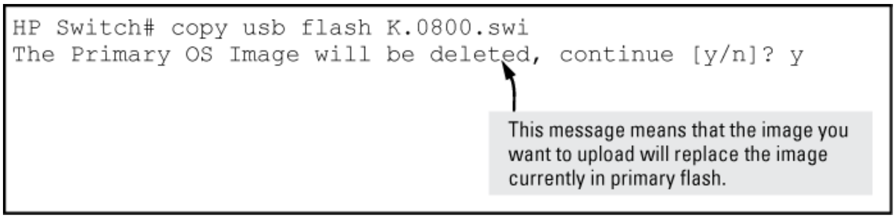
This command automatically downloads a switch software file to primary or secondary flash. If you do not specify the flash destination, the USB download defaults to primary flash.

Example

To copy a switch software file named `k0800.swi` from a USB device to primary flash:

1. Execute `copy` as shown below:

Figure 144 The command to copy switch software from USB



```
HP Switch# copy usb flash K.0800.swi
The Primary OS Image will be deleted, continue [y/n]? y
```

This message means that the image you want to upload will replace the image currently in primary flash.

When the switch finishes copying the software file from the USB device, it displays this progress message:

Validating and Writing System Software to the Filesystem....

2. When the copy finishes, you must reboot the switch to implement the newly loaded software. To do so, use one of the following commands

Syntax:

```
boot system flash[  primary | secondary  ]
```

Boots from the selected flash.

Syntax:

```
reload
```

Boots from the flash image and startup-config file. A switch covered in this guide (with multiple configuration files), also uses the current startup-config file.

For more information on these commands, see "Rebooting the Switch" in the *Basic Operation Guide* for your switch.

3. To confirm that the software downloaded correctly, execute `show system` and check the **Firmware revision** line.

Switch-to-switch download

You can use TFTP to transfer a software image between two switches of the same series. The CLI enables all combinations of flash location options. The menu interface enables you to transfer primary-to-primary or secondary-to-primary.

Downloading the OS from another switch (CLI)

Where two switches in your network belong to the same series, you can download a software image between them by initiating a `copy tftp` command from the destination switch. The options for this CLI feature include:

- Copy from primary flash in the source to either primary or secondary in the destination.
- Copy from either primary or secondary flash in the source to either primary or secondary flash in the destination.

Downloading from primary only (CLI)

Syntax:

```
copy tftp flash ip-addr flash[ primary | secondary ][oobm]
```

When executed in the destination switch, downloads the software flash in the source switch's primary flash to either the primary or secondary flash in the destination switch.

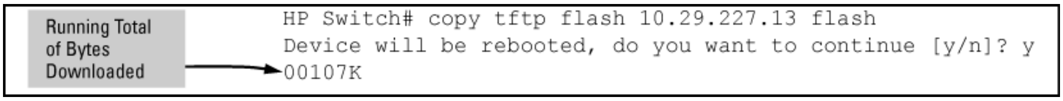
For switches that have a separate OOBM port, the `oobm` parameter specifies that the TFTP traffic must come in through the OOBM interface. If this parameter is not specified, the TFTP traffic comes in through the data interface. The `oobm` parameter is not available on switches that do not have a separate OOBM port. For more information on OOBM, see Appendix J, "Network Out-of-Band Management (OOBM) for the 6600 Switch" (page 492) in this guide.

If you do not specify either a primary or secondary flash location for the destination, the download automatically goes to primary flash.

Example

To download a software file from primary flash in a switch with an IP address of 10.29.227.103 to the primary flash in the destination switch, you would execute the following command in the destination switch's CLI:

Figure 145 Switch-to-switch, from primary in source to either flash in destination



```
HP Switch# copy tftp flash 10.29.227.13 flash
Device will be rebooted, do you want to continue [y/n]? y
00107K
```

Downloading from either flash in the source switch to either flash in the destination switch (CLI)

Syntax:

```
copy tftp flash ip-addr  /os/primary  |  /os/secondary  [ primary |
secondary ][oobm]
```

This command (executed in the destination switch) gives you the most options for downloading between switches. If you do not specify either a primary or secondary flash location for the destination, the download automatically goes to primary flash.

For switches that have a separate out-of-band management port, the `oobm` parameter specifies that the TFTP traffic must come in through the out-of-band management interface. If this parameter is not specified, the TFTP traffic comes in through the data interface. The `oobm` parameter is not available on switches that do not have a separate out-of-band management port. For more information on out-of-band management, see Appendix J, "Network Out-of-Band Management (OOBM) for the 6600 Switch" (page 492) in this guide.

Example

To download a software file from secondary flash in a switch with an IP address of 10.28.227.103 to the secondary flash in a destination switch, you would execute the following command in the destination switch's CLI:

Example 58 Switch-to-switch, from either flash in source to either flash in destination

```
HP Switch# copy tftp flash 10.29.227.13 flash /os/secondary secondary
Device will be rebooted, do you want to continue [y/n]? y
00184K
```

Switch-to-switch download to primary flash (Menu)

Using the menu interface, you can download a switch software file from either the primary or secondary flash of one switch to the primary flash of another switch of the same series.

1. From the switch console Main Menu in the switch to receive the download, select **7. Download OS** screen.
2. Ensure that the **Method** parameter is set to **TFTP** (the default).
3. In the **TFTP Server** field, enter the IP address of the remote switch containing the software file you want to download.
4. For the **Remote File Name**, enter one of the following:
   - To download the software in the primary flash of the source switch, enter `flash` in lowercase characters.
   - To download the software in the secondary flash of the source switch, enter `/os/secondary`.
5. Press **[Enter]**, and then **[X]** (for **eXecute**) to begin the software download.

   A "progress" bar indicates the progress of the download. When the entire switch software download has been received, all activity on the switch halts and the following messages appear:

   Validating and writing system software to FLASH...

6. After the primary flash memory has been updated with the new software, you must reboot the switch to implement the newly downloaded software. Return to the Main Menu and press **[6]** (for **Reboot Switch**). You then see this prompt:

   Continue reboot of system? : No

   Press the space bar once to change `No` to `Yes`, then press **[Enter]** to begin the reboot.

7. To confirm that the software downloaded correctly:
   a. From the Main Menu, select
      Status and Counters
      General System Information
   b. Check the **Firmware revision** line.

Copying software images

NOTE: For details on how switch memory operates, including primary and secondary flash, see “Switch Memory and Configuration” in the *Basic Operation Guide* for your switch.

TFTP: Copying a software image to a remote host (CLI)

Syntax:

`copy flash tftp` *`ip-addr filename`* [oobm]

Copies the primary flash image to a TFTP server.

For switches that have a separate OOBM port, the `oobm` parameter specifies that the transfer is through the OOBM interface. If this parameter is not specified, the transfer is through the data interface.

The `oobm` parameter is not available on switches that do not have a separate OOBM port. For more information on OOBM, see Appendix J, "Network Out-of-Band Management (OOBM) for the 6600 Switch" (page 492) in this guide.

Example

To copy the primary flash to a TFTP server having an IP address of 10.28.227.105:

```
HP Switch# copy flash tftp 10.28.227.105 k0800.swi
```

where `k0800.swi` is the filename given to the flash image being copied.

Xmodem: Copying a software image from the switch to a serially connected PC or UNIX workstation (CLI)

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation.

Syntax:

```
copy flash xmodem [[ pc] | unix  ]
```

Uses Xmodem to copy a designated configuration file from the switch to a PC or UNIX workstation.

Example

To copy the primary flash image to a serially connected PC:

1. Execute the following command:

   ```
   HP Switch# copy xmodem flash
   Press 'Enter' and start XMODEM on your host...
   ```

2. After you see the above prompt, press **[Enter]**.
3. Execute the terminal emulator commands to begin the file transfer.

USB: Copying a software image to a USB device (CLI)

To use this method, a USB flash memory device must be connected to the switch's USB port.

Syntax:

```
copy flash usb filename
```

Uses the USB port to copy the primary flash image from the switch to a USB flash memory device.

Example

To copy the primary image to a USB flash drive:

1. Insert a USB device into the switch's USB port.
2. Execute the following command:

   ```
   HP Switch# copy flash usb k0800.swi
   ```

   where `k0800.swi` is the name given to the primary flash image that is copied from the switch to the USB device.

Transferring switch configurations

For more information, see "About transferring switch configurations" (page 314).

TFTP: Copying a configuration file to a remote host (CLI)

Syntax:

```
copy  startup-config | running-config  tftp ip-addr remote-file [ pc
| unix ][oobm]
```

copy config *filename* tftp *ip-addr remote-file* [pc | unix] [oobm]

This command can copy a designated config file in the switch to a TFTP server. For more information, see "Multiple Configuration Files" in the *Basic Operation Guide* for your switch.

For switches that have a separate OOBM port, the `oobm` parameter specifies that the transfer is through the OOBM interface. If this parameter is not specified, the transfer is through the data interface.

The `oobm` parameter is not available on switches that do not have a separate OOBM port. For more information, see Appendix J, "Network Out-of-Band Management (OOBM) for the 6600 Switch" (page 492) in this guide.

Example

To upload the current startup configuration to a file named **`sw8200`** in the configs directory on drive **"d"** in a TFTP server having an IP address of 10.28.227.105:

```
ProCurve# copy startup-config tftp 10.28.227.105
   d:\configs\sw8200
```

TFTP: Copying a configuration file from a remote host (CLI)

Syntax:

copy tftp startup-config | running-config *ip-addr remote-file* [pc | unix] [oobm]
copy tftp config *filename ip-addr remote-file* [pc | unix] [oobm]

This command can copy a configuration from a remote host to a designated config file in the switch. For more information, see "Multiple Configuration Files" in the *Basic Operation Guide* for your switch.

For more information on flash image use, see "Using Primary and Secondary Flash Image Options" in the *Basic Operation Guide* for your switch.

For switches that have a separate OOBM port, the `oobm` parameter specifies that the transfer is through the OOBM interface. If this parameter is not specified, the transfer is through the data interface.

The `oobm` parameter is not available on switches that do not have a separate OOBM port. For more information, see Appendix J, "Network Out-of-Band Management (OOBM) for the 6600 Switch" (page 492) in this guide.

Example

To download a configuration file named **`sw8200`** in the **`configs`** directory on drive **"d"** in a remote host having an IP address of 10.28.227.105:

```
HP Switch# copy tftp startup-config 10.28.227.105
   d:\configs\sw8200
```

TFTP: Copying a customized command file to a switch (CLI)

Using the `copy tftp` command with the `show-tech` option provides the ability to copy a customized command file to the switch. When the `show tech custom` command is executed, the commands in the custom file are executed instead of the hard-coded list of commands. If no custom file is found, the current hard-coded list is executed. This list contains commands to display data, such as the image stamp, running configuration, boot history, port settings, and so on.

Syntax:

copy tftp show-tech ipv4 or ipv6 address *filename* [oobm]

Copies a customized command file to the switch (see Example 59 (page 297)).

For switches that have a separate OOBM port, the `oobm` parameter specifies that the transfer is through the out-of-band management interface. If this parameter is not specified, the transfer is through the data interface. The `oobm` parameter is not available on switches that do not have a separate OOBM port. For more information, see Appendix J, "Network Out-of-Band Management (OOBM) for the 6600 Switch" (page 492) in this guide.

Example

Example 59 Using the `copy tftp show-tech` command to upload a customized command file

```
HP Switch(config)# copy tftp show-tech 10.10.10.3 commandfile1
```

Syntax:

`show tech custom`

Executes the commands found in a custom file instead of the hard-coded list.

NOTE: Exit the global config mode (if needed) before executing `show tech` commands.

Example

Example 60 The `show tech custom` command

You can include `show tech` commands in the custom file, with the exception of `show tech custom`. For example, you can include the command `show tech all`.

If no custom file is found, a message displays stating "No SHOW-TECH file found." (No custom file was uploaded with the `copy tftp show-tech` command.)

```
HP Switch# show tech custom
No SHOW-TECH file found.
```

Xmodem: Copying a configuration file to a serially connected PC or UNIX workstation (CLI)

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation. You will need to:

- Determine a filename to use.
- Know the directory path you will use to store the configuration file.

Syntax:

```
copy [  startup-config | running-config  ] xmodem [  pc | unix  ]
copy config filename xmodem  pc | unix
```

Uses Xmodem to copy a designated configuration file from the switch to a PC or UNIX workstation. For more information, see "Multiple Configuration Files" in the *Basic Operation Guide* for your switch.

Example

To copy a configuration file to a PC serially connected to the switch:

1. Determine the file name and directory location on the PC.
2. Execute the following command:

   ```
   HP Switch# copy startup-config xmodem pc
   Press 'Enter' and start XMODEM on your host...
   ```

3. After you see the above prompt, press **[Enter]**.
4. Execute the terminal emulator commands to begin the file transfer.

Xmodem: Copying a configuration file from a serially connected PC or UNIX workstation (CLI)

To use this method, the switch must be connected via the serial port to a PC or UNIX workstation on which is stored the configuration file you want to copy. To complete the copying, you need to know the name of the file to copy and the drive and directory location of the file.

Syntax:

```
copy xmodem startup-config [  pc | unix  ]
copy xmodem config filename  [  pc | unix  ]
```

Copies a configuration file from a serially connected PC or UNIX workstation to a designated configuration file on the switch. For more information, see "Multiple Configuration Files" in the *Basic Operation Guide* for your switch.

Example

To copy a configuration file from a PC serially connected to the switch:

1. Execute the following command:

   ```
   HP Switch# copy xmodem startup-config pc
   Device will be rebooted, do you want to continue [y/n]? y
   Press 'Enter' and start XMODEM on your host...
   ```

2. After you see the above prompt, press **[Enter]**.
3. Execute the terminal emulator commands to begin the file transfer.
4. When the download finishes, you must reboot the switch to implement the newly downloaded software. To do so, use one of the following commands:

   #### Syntax:

   ```
   boot system flash [ primary | secondary ]
   boot system flash [config filename ]
   ```

   Switches boot from the designated configuration file. For more information, see "Multiple Configuration Files" in the *Basic Operation Guide* for your switch.

   #### Syntax:

   ```
   reload
   ```

   Reboots from the flash image currently in use.

   (For more on these commands, see "Rebooting the Switch" in the *Basic Operation Guide* for your switch..)

USB: Copying a configuration file to a USB device (CLI)

To use this method, a USB flash memory device must be connected to the switch's USB port.

Syntax:

```
copy startup-config usb filename
copy running-config usb filename
```

Uses the USB port to copy a designated configuration file from the switch to a USB flash memory device. For more information, see "Multiple Configuration Files" in the *Basic Operation Guide* for your switch.

Example

To copy the startup configuration file to a USB flash drive:

1. Insert a USB device into the switch's USB port.

2. Execute the following command:

   ```
   HP Switch# copy startup-config usb HP Switch-config
   ```

   where `HP Switch-config` is the name given to the configuration file that is copied from the switch to the USB device.

USB: Copying a configuration file from a USB device (CLI)

To use this method, the switch must be connected via the USB port to a USB flash drive on which is stored the configuration file you want to copy. To execute the command, you will need to know the name of the file to copy.

Syntax:

```
copy usb startup-config filename
```

Copies a configuration file from a USB device to the startup configuration file on the switch.

Example

To copy a configuration file from a USB device to the switch:

1. Insert a USB device into the switch's USB port.
2. Execute the following command:

   ```
   HP Switch# copy usb startup-config HP Switch-config
   ```

   where `HP Switch-config` is the name of the file to copy.
3. At the prompt, press **[Enter]** to reboot the switch and implement the newly downloaded software.

Transferring ACL command files

TFTP: Uploading an ACL command file from a TFTP server (CLI)

Syntax:

```
copy tftp command-file ip-addr filename.txt  unix | pc [oobm]
```

Copies and executes the named text file from the specified TFTP server address and executes the ACL commands in the file.

`ip-addr`	The IP address of a TFTP server available to the switch
`filename.txt`	A text file containing ACL commands and stored in the TFTP directory of the server identified by *`ip-addr`*
`[  unix | pc  ]`	The type of workstation used for serial, Telnet, or SSH access to the switch CLI
`[oobm]`	For switches that have a separate out-of-band management port, specifies that the transfer will be through the out-of-band management interface. (Default is transfer through the data interface.)

Depending on the ACL commands used, this action does one of the following in the `running-config` file:

- Creates a new ACL.
- Replaces an existing ACL. (See "Creating an ACL Offline" in the "Access Control Lists (ACLs)" chapter in the latest Access Security Guide for your switch.)
- Adds to an existing ACL.

Example

Suppose you:

1. Created an ACL command file named **`vlan10_in.txt`** to update an existing ACL.
2. Copied the file to a TFTP server at 18.38.124.16.

Using a PC workstation, you then execute the following from the CLI to upload the file to the switch and implement the ACL commands it contains:

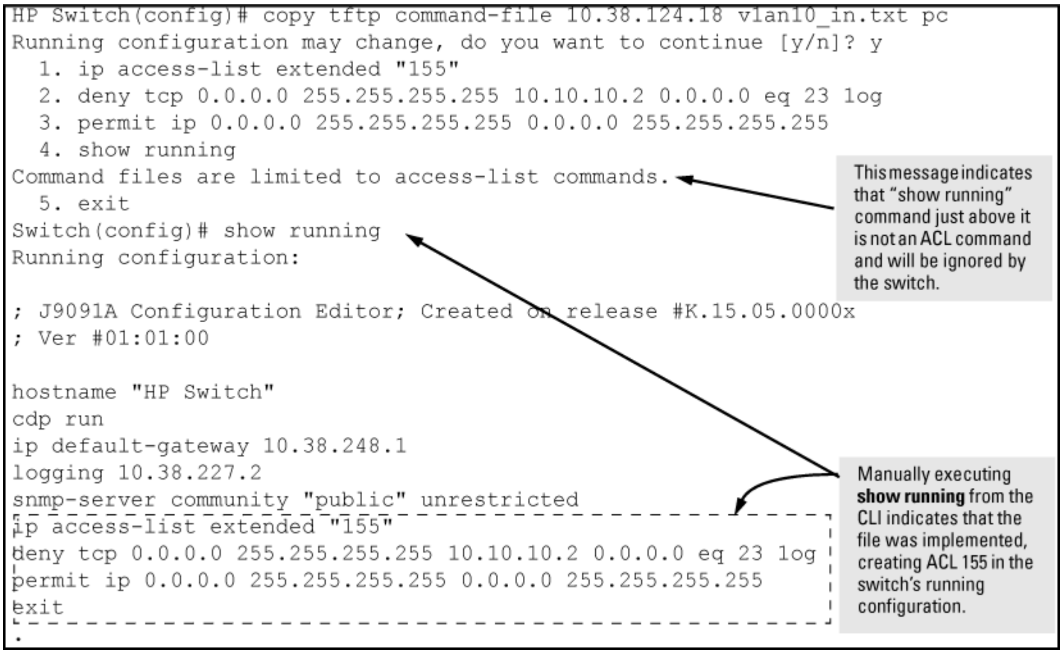
```
HP Switch(config)# copy tftp command-file 18.38.124.16
vlan10_in.txt pc
```

The switch displays this message:

```
Running configuration may change, do you want to continue
[y/n]?
```

To continue with the upload, press the **[Y]** key. To abort the upload, press the **[N]** key. Note that if the switch detects an illegal (non-ACL) command in the file, it bypasses the illegal command, displays a notice (as shown in Figure 146 (page 300)), and continues to implement the remaining ACL commands in the file.

Figure 146 Using the `copy` command to download and configure an ACL



```
HP Switch(config)# copy tftp command-file 10.38.124.18 vlan10_in.txt pc
Running configuration may change, do you want to continue [y/n]? y
  1. ip access-list extended "155"
  2. deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
  3. permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  4. show running
Command files are limited to access-list commands.
  5. exit
Switch(config)# show running
Running configuration:

; J9091A Configuration Editor; Created on release #K.15.05.0000x
; Ver #01:01:00

hostname "HP Switch"
cdp run
ip default-gateway 10.38.248.1
logging 10.38.227.2
snmp-server community "public" unrestricted
ip access-list extended "155"
deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
.
```

This message indicates that "show running" command just above it is not an ACL command and will be ignored by the switch.

Manually executing **show running** from the CLI indicates that the file was implemented, creating ACL 155 in the switch's running configuration.

Xmodem: Uploading an ACL command file from a serially connected PC or UNIX workstation (CLI)

Syntax:

```
copy xmodem command-file [  unix | pc  ]
```

Uses Xmodem to copy and execute an ACL command from a PC or UNIX workstation. Depending on the ACL commands used, this action does one of the following in the running-config file:

- Creates a new ACL.
- Replaces an existing ACL. (See "Creating an ACL Offline" in the "Access Control Lists (ACLs)" chapter in the latest *Access Security Guide* for your switch.)
- Adds to an existing ACL.

USB: Uploading an ACL command file from a USB device (CLI)

Syntax:

```
copy usb command-file filename.txt [  unix | pc  ]
```

Copies and executes the named text file from a USB flash drive and executes the ACL commands in the file.

`filename.txt`	A text file containing ACL commands and stored in the USB flash drive
`unix | pc`	The type of workstation used to create the text file.

Depending on the ACL commands used, this action does one of the following in the running-config file:

- Creates a new ACL.
- Replaces an existing ACL. (See "Creating an ACL Offline" in the "Access Control Lists (ACLs)" chapter in the latest Access Security Guide for your switch.)
- Adds to an existing ACL.

Example

Suppose you:

1. Created an ACL command file named **`vlan10_in.txt`** to update an existing ACL.
2. Copied the file to a USB flash drive.

Using a PC workstation, you then execute the following from the CLI to upload the file to the switch and implement the ACL commands it contains:

```
HP Switch(config)# copy usb command-file vlan10_in.txt pc
```

The switch displays this message:

```
Running configuration may change, do you want to continue
[y/n]?
```

To continue with the upload, press the **[Y]** key. To abort the upload, press the **[N]** key. Note that if the switch detects an illegal (non-ACL) command in the file, it bypasses the illegal command, displays a notice (as in the tftp example shown in Figure 146 (page 300)), and continues to implement the remaining ACL commands in the file.

Copying diagnostic data to a remote host, USB device, PC, or UNIX workstation

Copying command output to a destination device (CLI)

Syntax:

```
copy command-output "cli-command" tftp ip-address
filepath-filename [oobm]
copy command-output "cli-command" usb filename
copy command-output "cli-command" xmodem
```

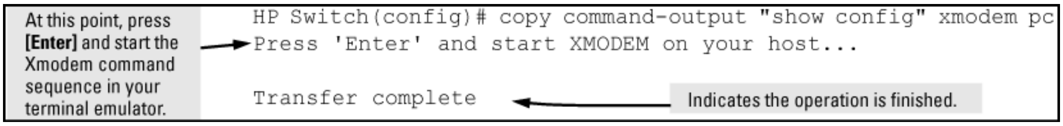
These commands direct the displayed output of a CLI command to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.

For switches that have a separate OOBM port, the `oobm` parameter specifies that the transfer is through the OOBM interface. If this parameter is not specified, the transfer is through the data interface. The `oobm` parameter is not available on switches that do not have a separate OOBM port. For more information on out-of-band management, see Appendix J, "Network Out-of-Band Management (OOBM) for the 6600 Switch" (page 492) in this guide.

Example

To use Xmodem to copy the output of `show config` to a serially connected PC:

Figure 147 Sending command output to a file on an attached PC



```
HP Switch(config)# copy command-output "show config" xmodem pc
Press 'Enter' and start XMODEM on your host...

Transfer complete
```

At this point, press **[Enter]** and start the Xmodem command sequence in your terminal emulator.

Indicates the operation is finished.

NOTE: The command you specify must be enclosed in double quotation marks.

Copying Event Log output to a destination device (CLI)

Syntax:

```
copy event-log smm [ tftp | usb | xmodem ]
copy event-log tftp ip-address filepath_filename  [oobm]
copy event-log usb filename
copy event-log xmodem filename
```

These commands copy the Event Log content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.

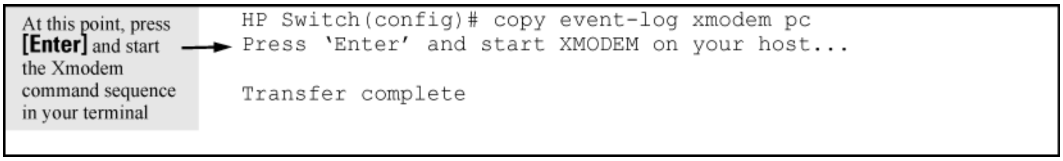
When used with the `smm` option, the entire Event Log, both active management module events and standby management module events, is copied to the selected host, USB device, or serially connected PC or UNIX workstation.

For switches that have a separate OOBM port, the `oobm` parameter specifies that the transfer is through the OOBM interface. If this parameter is not specified, the transfer is through the data interface. The `oobm` parameter is not available on switches that do not have a separate OOBM port. For more information on OOBM, see Appendix J, "Network Out-of-Band Management (OOBM) for the 6600 Switch" (page 492) in this guide.

Example

To copy the event log to a PC connected to the switch:

Figure 148 Sending event log content to a file on an attached PC



```
HP Switch(config)# copy event-log xmodem pc
Press 'Enter' and start XMODEM on your host...

Transfer complete
```

At this point, press **[Enter]** and start the Xmodem command sequence in your terminal

Copying crash data content to a destination device (CLI)

This command uses TFTP, USB, or Xmodem to copy the Crash Data content to a destination device. You can copy individual slot information or the management module's switch information. If you do not specify either, the command defaults to the management function's data.

Syntax:

```
copy crash-data [  slot-id | master  ]
tftp ip-address filename  [oobm]
copy crash-data [  slot-id | mm  ]
```

```
usb filename
copy crash-data [  slot-id | mm  ]
xmodem
```

These commands copy the crash data content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation.

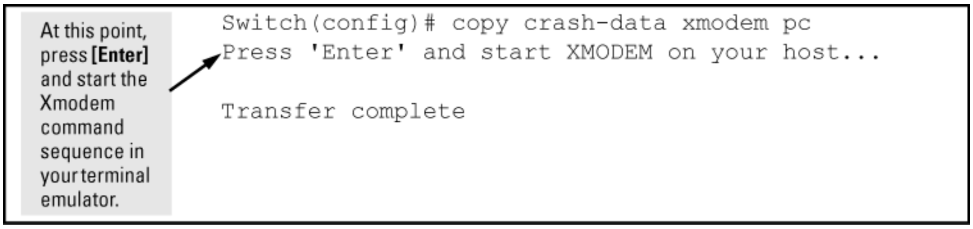
`slot-id`	a - h—Retrieves the crash log or crash data from the processor on the module in the specified slot
`mm`	Retrieves crash log or crash data from the switch's chassis processor. When "mm" is specified, crash files from both management modules are copied.
`oobm`	For switches that have a separate OOBM port, specifies that the transfer is through the OOBM interface. (Default is transfer through the data interface.)

You can copy individual slot information or the management module (mm) switch information. If you do not specify either, the command defaults to the mm data.

Example

To copy the switch's crash data to a file in a PC:

Figure 149 Copying switch crash data content to a PC



At this point, press **[Enter]** and start the Xmodem command sequence in your terminal emulator.

```
Switch(config)# copy crash-data xmodem pc
Press 'Enter' and start XMODEM on your host...

Transfer complete
```

Copying crash data with redundant management (CLI)

When you use redundant management, the `copy crash-data` command operates somewhat differently:

Syntax:

```
copy crash-data [  slot-id  | mm ] tftp ip-address filename
[oobm]
```

Copies the crash data of both the active and standby management modules to a user-specified file. If no parameter is specified, files from all modules (management and interface) are concatenated.

`slot-id`	Retrieves the crash data from the module in the specified slot.
`mm`	Retrieves the crash data from both management modules and concatenates them.
`oobm`	For switches that have a separate OOBM port, specifies that the transfer is through the OOBM interface. (Default is transfer through the data interface.)

Copying crash log data content to a destination device (CLI)

Syntax:

```
copy crash-log [  slot-id | mm  ] tftp ip-address filepath and
filename  [oobm]
```

```
copy crash-log [ slot-id | mm ] usb filename
copy crash-log [ slot-id | mm ] xmodem
```

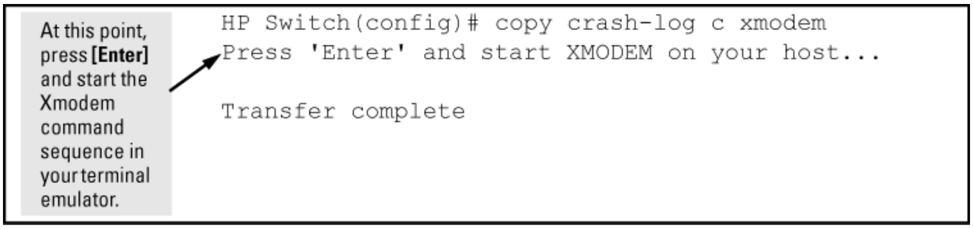
These commands copy the Crash Log content to a remote host, attached USB device, or to a serially connected PC or UNIX workstation. You can copy individual slot information or the management module (mm) switch information.

`slot-id`	a - h—Retrieves the crash log from the processor on the module in the specified slot
`mm`	Retrieves the crash log from the switch's chassis processor. When mm is specified, crash files from both management modules are copied.
`oobm`	For switches that have a separate OOBM port, specifies that the transfer is through the OOBM interface. (Default is transfer through the data interface.) If you do not specify either, the command defaults to the mm data.

Example

To copy the crash log for slot C to a file in a PC connected to the switch:

Figure 150 Sending a crash log for slot C to a file on an attached PC



At this point, press **[Enter]** and start the Xmodem command sequence in your terminal emulator.

```
HP Switch(config)# copy crash-log c xmodem
Press 'Enter' and start XMODEM on your host...

Transfer complete
```

Copying crash logs with redundant management (8200zl) (CLI)

When you use redundant management, the `copy crash-log` command operates somewhat differently.

Syntax:

```
copy crash-log [ slot-id | mm ] tftp ip-address filepath and
filename [oobm]
```

Copies the crash logs of both the active and standby management modules to a user-specified file. If no parameter is specified, files from all modules (management and interface) are concatenated.

`slot-id`	Retrieves the crash log from the module in the specified slot.
`mm`	Retrieves the crash logs from both management modules and concatenates them.
`oobm`	For switches that have a separate OOBM port, specifies that the transfer is through the OOBM interface. (Default is transfer through the data interface.)

Copying coredumps from the standby management module (8200zl switches)

It is important that the coredump files on the standby management module are accessible for diagnostic purposes.

Syntax:

```
copy core-dump [ mm usb filename  | standby flash | usb
filename  ]
```

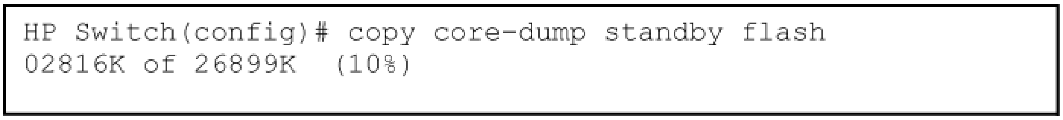
Copies the management module coredump or the standby management module coredump to the active management module flash or to a USB flash drive (see Figure 151 (page 305)).

`flash`	Copies the core file of the standby management module to the flash of the active management module. The destination file is fixed as `dumpM1.cor` or `dumpM2.cor`, depending on which module is the standby management module.
`usb` *`filename`*	Copies the management module's core file or the standby management module's core file to a USB flash drive. The optional filename defaults to `dumpM1.cor` or `dumpM2.cor`, depending on which module is the standby management module

While the file is being copied, the number of bytes transferred and the percentage of the total is displayed. Management module core files can be quite large. Use **Cntl-C** to cleanly cancel the transfer.

Example

Figure 151 Copying the standby coredump to flash



```
HP Switch(config)# copy core-dump standby flash
02816K of 26899K  (10%)
```

If there is no coredump on the standby management module, the following error message displays:

```
Standby MM coredump does not exist.
```

If there is not enough destination space before or during the transfer to flash or USB, the following error message displays:

```
Insufficient FLASH space to complete the file copy.
```

Flight data recorder

The Flight Data Recorder (FDR) log collects information that is "interesting" when the switch is not performing correctly, but has not crashed. Runtime logs are written to FDR memory while the switch is running, and crashtime logs are collected and stored in the FDR buffer during a switch crash.

Syntax:

```
copy fdr-log [[slot slot-list] | [mm-active [[current] | [previous]]]
| [mm-standby] | [all]]
tftp [[hostname] | [ip-addr]]
filename
```

Copies `fdr-log` files to a user-specified file.

`all`	Copies all the log files from both management modules and all slots.
`mn-active`	Copies the active management module's log.
`mn-standby`	Copies the standby management module's log.
`slot`	Retrieves the crash log from the module in the identified slots.

Enabling or disabling the USB port with the CLI

This feature allows configuration of the USB port with either the CLI or SNMP.

Syntax:

```
usb-port
no usb-port
```

Enables the USB port. The no form of the command disables the USB port and any access to the device.

Viewing the status of the USB port (CLI)

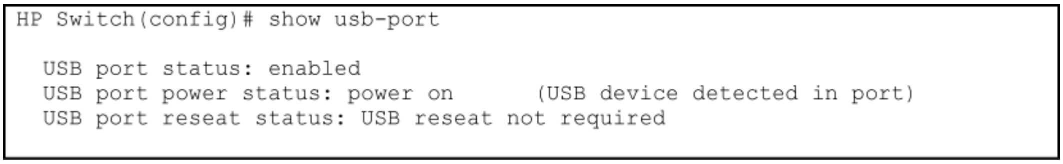
Syntax:

```
show usb-port
```

Displays the status of the USB port. It can be enabled, disabled, or not present. (See Figure 152 (page 306) or Figure 153 (page 306), depending on your version.)

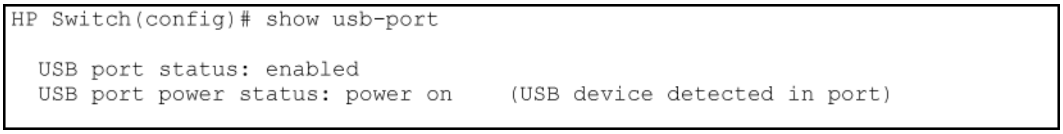
Example

Figure 152 `show usb-port` **command output on version K.13.59 and later**



```
HP Switch(config)# show usb-port

  USB port status: enabled
  USB port power status: power on      (USB device detected in port)
  USB port reseat status: USB reseat not required
```

Figure 153 `show usb-port` **command output on version K.14.XX**



```
HP Switch(config)# show usb-port

  USB port status: enabled
  USB port power status: power on    (USB device detected in port)
```

One of the following messages indicates the presence or absence of the USB device:

- Not able to sense device in USB port
- USB device detected in port
- No USB device detected in port

The reseat status messages can be one of the following (K.13.XX only):

- Undetermined USB reseat requirement
- USB reseat not required
- USB device reseat required for USB autorun

The autorun feature works only when a USB device is inserted and the USB port is enabled.

Using USB autorun

For more information, see “About using USB autorun” (page 316).

The general process for using USB autorun is as follows (*steps 1, 2, and 7 require an upcoming update to PCM+, as described above*):

1. Create an AutoRun file using PCM+.

   See the HP Switch Manager documentation for details.

   NOTE: Creating the AutoRun file in PCM+ includes the following steps:

   - **a.** Specify the target device or devices.
     b. Create the CLI script to be executed on the target devices.
     c. Determine if the file will be signed and/or encrypted.
     d. Determine if the file will be 'run once' (moved to a 'processed' directory on execution) or 'run many' (kept in the root directory of the flash drive from where it can be executed again).

2. Deploy the AutoRun file to a USB flash drive.
3. (If required) Enable the autorun feature on the switch (autorun is enabled by default unless an operator or manager password has been set—See "Autorun and configuring passwords" (page 318)).
4. (If the AutoRun file has been signed or encrypted) Enable secure-mode on the switch:
   a. Configure an encryption key and a valid trusted certificate
   b. Enable secure-mode via the CLI.

   See "About downloading switch software" (page 308).
5. Insert the USB flash drive into the switch's USB auxiliary port.

   The switch processes the AutoRun file automatically and writes a result (.txt) file and report (.xml) file back to the USB flash drive, reporting on the command operations that were executed.
6. Remove the USB device from the USB port.

   The switch executes any post-commands, such as rebooting the switch to apply any configuration updates.
7. (Optional) Transfer the 'result file' and 'report file' to a PCM+-enabled computer for report checking.

   See "Troubleshooting autorun operations" (page 316).

Configuring autorun on the switch (CLI)

Syntax:

`[ no ] autorun [ encryption-key` *`key-string`* `| secure-mode ]`

When executed from the configuration mode, enables or disables USB autorun on the switch.

Use the `encryption-key` keyword to configure or remove an encryption-key (a base-64 encoded string). The encryption key is a prerequisite for enabling autorun in secure-mode. Encryption is regarded only when the AutoRun file is also signed by an authentic source.

Use the `secure-mode` keyword to enable or disable secure mode for autorun.

(Default: Enabled—or disabled if a password has been set)

For information about enabling secure mode on autorun, see "Autorun secure mode" (page 317).

Viewing autorun configuration information

The `show autorun` command displays autorun configuration status information, as shown in the following example.

```
HP Switch(config)# show autorun

 Autorun configuration status
```

```
    Enabled        : Yes
    Secure-mode    : Disabled
    Encryption-key :
```

About downloading switch software

HP Switch periodically provides switch software updates through the HP Switch Networking website. For more information, see the support and warranty booklet shipped with the switch, or visit www.procurve.com and click on **software updates**.

NOTE: This manual uses the terms *switch software and software image* to refer to the downloadable software files the switch uses to operate its networking features. Other terms sometimes include *Operating System, or OS*.

General software download rules

- Switch software that you download via the menu interface always goes to primary flash.
- After a software download, you must reboot the switch to implement the new software. Until a reboot occurs, the switch continues to run on the software it was using before the download.

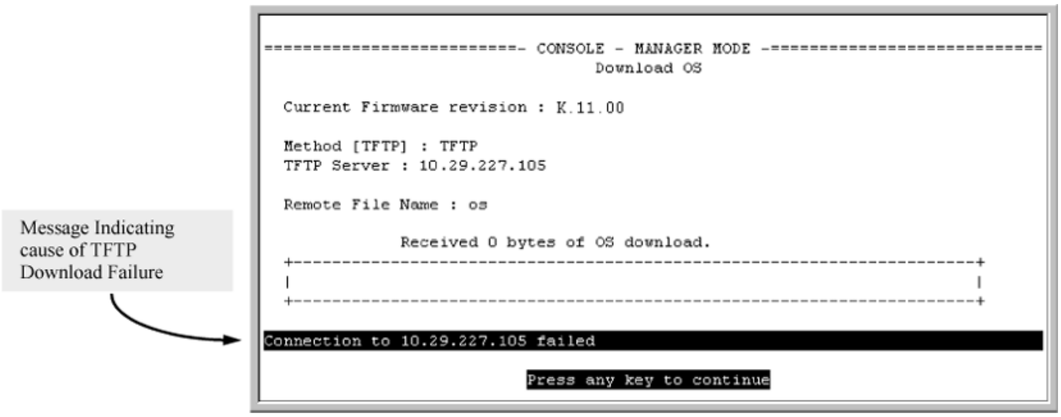
NOTE: Downloading new switch software does not change the current switch configuration. The switch configuration is contained in separate files that can also be transferred. See "Transferring switch configurations" (page 295).

In most cases, if a power failure or other cause interrupts a flash image download, the switch reboots with the image previously stored in primary flash. In the unlikely event that the primary image is corrupted (which may occur if a download is interrupted by a power failure), the switch goes into boot ROM mode. In this case, use the boot ROM console to download a new image to primary flash.

Troubleshooting TFTP download failures

When using the menu interface, if a TFTP download fails, the Download OS (Operating System, or software) screen indicates the failure (see Figure 154 (page 308)).

Figure 154 Example of message for download failure



```
=========================- CONSOLE - MANAGER MODE -===========================
                                Download OS

  Current Firmware revision : K.11.00

  Method [TFTP] : TFTP
  TFTP Server : 10.29.227.105

  Remote File Name : os

                Received 0 bytes of OS download.
  +----------------------------------------------------------------------+
  |                                                                      |
  +----------------------------------------------------------------------+

Connection to 10.29.227.105 failed

                             Press any key to continue
```

Message Indicating cause of TFTP Download Failure

Some of the causes of download failures include:

- Incorrect or unreachable address specified for the **TFTP Server** parameter. This may include network problems.
- Incorrect VLAN.
- Incorrect name specified for the **Remote File Name** parameter, or the specified file cannot be found on the TFTP server. This can also occur if the TFTP server is a UNIX machine and the case (upper or lower) for the filename on the server does not match the case for the filename entered for the **Remote File Name** parameter in the **Download OS** (Operating System, or software) screen.

- One or more of the switch's IP configuration parameters are incorrect.
- For a UNIX TFTP server, the file permissions for the software file do not allow the file to be copied.
- Another console session (through either a direct connection to a terminal device or through Telnet) was already running when you started the session in which the download was attempted.

To find more information on the cause of a download failure:

- Examine the messages in the switch's Event Log by executing the `show log tftp` command from the CLI.
- For more on the Event Log, see "Using the Event Log for troubleshooting switch problems" (page 414).
- For descriptions of individual Event Log messages, see the latest version of the *Event Log Message Reference Guide* for your switch, available on the HP Switch website. (See "Getting Documentation From the Web".)

NOTE: If an error occurs in which normal switch operation cannot be restored, the switch automatically reboots itself, and an appropriate message is displayed after the reboot.

Using SCP and SFTP

For some situations you may want to use a secure method to issue commands or copy files to the switch. By opening a secure, encrypted SSH session and enabling ip ssh file transfer, you can then use a third-party software application to take advantage of SCP and SFTP. SCP and SFTP provide a secure alternative to TFTP for transferring information that may be sensitive (like switch configuration files) to and from the switch. Essentially, you are creating a secure SSH tunnel as a way to transfer files with SFTP and SCP channels.

Once you have configured your switch to enable secure file transfers with SCP and SFTP, files can be copied to or from the switch in a secure (encrypted) environment and TFTP is no longer necessary.

To use these commands, you must install on the administrator workstation a third-party application software client that supports the SFTP and/or SCP functions. Some examples of software that supports SFTP and SCP are PuTTY, Open SSH, WinSCP, and SSH Secure Shell. Most of these are freeware and may be downloaded without cost or licensing from the internet. There are differences in the way these clients work, so be sure you also download the documentation.

As described earlier in this chapter you can use a TFTP client on the administrator workstation to update software images. This is a plain-text mechanism that connects to a standalone TFTP server or another HP switch acting as a TFTP server to obtain the software image files. Using SCP and SFTP allows you to maintain your switches with greater security. You can also roll out new software images with automated scripts that make it easier to upgrade multiple switches simultaneously and securely.

SFTP is unrelated to FTP, although there are some functional similarities. Once you set up an SFTP session through an SSH tunnel, some of the commands are the same as FTP commands. Certain commands are not allowed by the SFTP server on the switch, such as those that create files or folders. If you try to issue commands such as `create` or `remove` using SFTP, the switch server returns an error message.

You can use SFTP just as you would TFTP to transfer files to and from the switch, but with SFTP, your file transfers are encrypted and require authentication, so they are more secure than they would be using TFTP. SFTP works only with SSH version 2 (SSH v2).

NOTE: SFTP over SSH version 1 (SSH v1) is not supported. A request from either the client or the switch (or both) using SSH v1 generates an error message. The actual text of the error message differs, depending on the client software in use. Some examples are:

```
Protocol major versions differ: 2 vs. 1
Connection closed

Protocol major versions differ: 1 vs. 2
Connection closed

Received disconnect from  ip-addr : /usr/local/libexec/
sftp-server: command not supported
Connection closed
```

SCP is an implementation of the BSD `rcp` (Berkeley UNIX remote copy) command tunneled through an SSH connection.

SCP is used to copy files to and from the switch when security is required. SCP works with both SSH v1 and SSH v2. Be aware that the most third-party software application clients that support SCP use SSHv1.

The general process for using SCP and SFTP involves three steps:

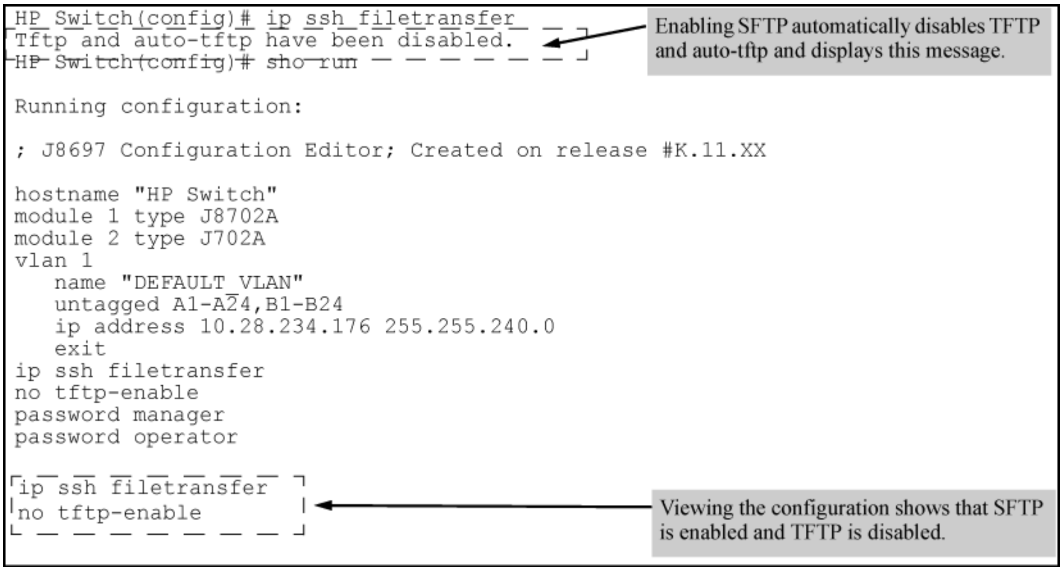
1. Open an SSH tunnel between your computer and the switch if you have not already done so.

   (This step assumes that you have already set up SSH on the switch.)
2. Execute `ip ssh filetransfer` to enable secure file transfer.
3. Use a third-party client application for SCP and SFTP commands.

Disabling TFTP and auto-TFTP for enhanced security

Using the `ip ssh filetransfer` command to enable SFTP automatically disables TFTP and auto-TFTP (if either or both are enabled), as shown in Figure 155 (page 310).

Figure 155 Example of switch configuration with SFTP enabled



```
HP Switch(config)# ip ssh filetransfer
Tftp and auto-tftp have been disabled.
HP Switch(config)# sho run

Running configuration:

; J8697 Configuration Editor; Created on release #K.11.XX

hostname "HP Switch"
module 1 type J8702A
module 2 type J702A
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A24,B1-B24
   ip address 10.28.234.176 255.255.240.0
   exit
ip ssh filetransfer
no tftp-enable
password manager
password operator

ip ssh filetransfer
no tftp-enable
```

Enabling SFTP automatically disables TFTP and auto-tftp and displays this message.

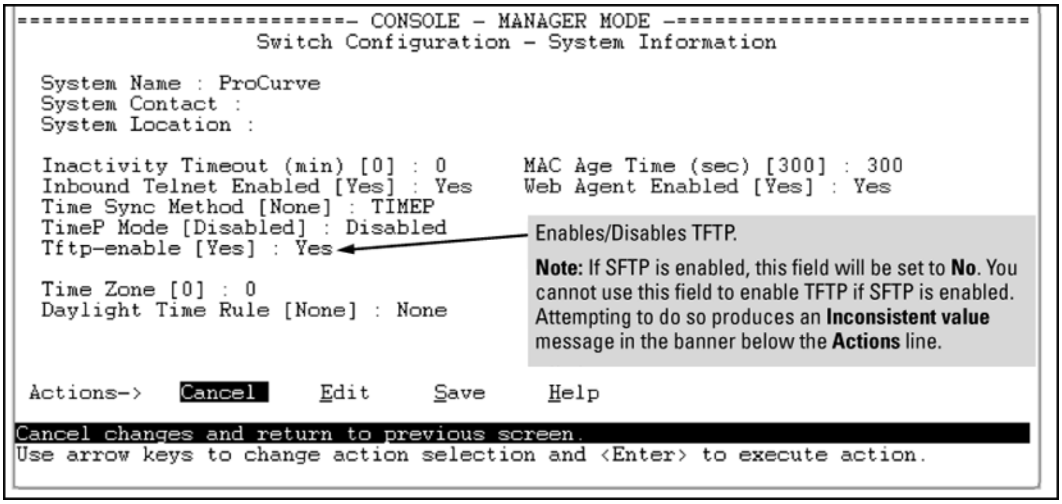
Viewing the configuration shows that SFTP is enabled and TFTP is disabled.

If you enable SFTP and then later disable it, TFTP and auto-TFTP remain disabled unless they are explicitly re-enabled.

Operating rules are:

- The TFTP feature is enabled by default, and can be enabled or disabled through the CLI, the Menu interface (see Figure 156 (page 311)), or an SNMP application. Auto-TFTP is disabled by default and must be configured through the CLI.

  Figure 156 Using the Menu interface to disable TFTP

  ```
  =========================- CONSOLE - MANAGER MODE -===========================
                     Switch Configuration - System Information

    System Name : ProCurve
    System Contact :
    System Location :

    Inactivity Timeout (min) [0] : 0      MAC Age Time (sec) [300] : 300
    Inbound Telnet Enabled [Yes] : Yes    Web Agent Enabled [Yes] : Yes
    Time Sync Method [None] : TIMEP
    TimeP Mode [Disabled] : Disabled
    Tftp-enable [Yes] : Yes

    Time Zone [0] : 0
    Daylight Time Rule [None] : None


   Actions->   Cancel     Edit     Save     Help

  Cancel changes and return to previous screen.
  Use arrow keys to change action selection and <Enter> to execute action.
  ```

  Enables/Disables TFTP.

  Note: If SFTP is enabled, this field will be set to **No**. You cannot use this field to enable TFTP if SFTP is enabled. Attempting to do so produces an **Inconsistent value** message in the banner below the **Actions** line.

- While SFTP is enabled, TFTP and auto-TFTP cannot be enabled from the CLI. Attempting to enable either non-secure TFTP option while SFTP is enabled produces one of the following messages in the CLI:

  ```
  SFTP must be disabled before enabling tftp.
  SFTP must be disabled before enabling auto-tftp.
  ```

  Similarly, while SFTP is enabled, TFTP cannot be enabled using an SNMP management application. Attempting to do so generates an "inconsistent value" message. (An SNMP management application cannot be used to enable or disable auto-TFTP.)

- To enable SFTP by using an SNMP management application, you must first disable TFTP and, if configured, auto-TFTP on the switch. You can use either an SNMP application or the CLI to disable TFTP, but you must use the CLI to disable auto-TFTP. The following CLI commands disable TFTP and auto-TFTP on the switch.

Enabling SSH V2 (required for SFTP)

```
HP Switch(config)# ip ssh version 2
```

NOTE: As a matter of policy, administrators should *not* enable the SSH V1-only or the SSH V1-or-V2 advertisement modes. SSHv1 is supported on only some legacy switches (such as the HP Switch Series 2500 switches).

Confirming that SSH is enabled

```
HP Switch(config)# show ip ssh
```

Once you have confirmed that you have enabled an SSH session (with the `show ip ssh` command), enter `ip ssh filetransfer` so that SCP and/or SFTP can run. You can then open your third-party software client application to begin using the SCP or SFTP commands to safely transfer files or issue commands to the switch.

NOTE: Any attempts to use SCP or SFTP without using `ip ssh filetransfer` cause the SCP or SFTP session to fail. Depending on the client software in use, you will receive an error message on the originating console, for example:

```
IP file transfer not enabled on the switch
```

Disabling secure file transfer

```
HP Switch(config)# no ip ssh filetransfer
```

Authentication

Switch memory allows up to ten public keys. This means the authentication and encryption keys you use for your third-party client SCP/SFTP software can differ from the keys you use for the SSH session, even though both SCP and SFTP use a secure SSH tunnel.

NOTE: SSH authentication is mutually exclusive with RADIUS servers.

Some clients, such as PSCP (PuTTY SCP), automatically compare switch host keys for you. Other clients require you to manually copy and paste keys to the **`$HOME/.ssh/known_hosts`** file. Whatever SCP/SFTP software tool you use, after installing the client software you must verify that the switch host keys are available to the client.

Because the third-party software utilities you may use for SCP/SFTP vary, you should refer to the documentation provided with the utility you select before performing this process.

SCP/SFTP operating notes

- When an SFTP client connects, the switch provides a file system displaying all of its available files and folders. No file or directory creation is permitted by the user. Files may be only uploaded or downloaded, according to the permissions mask. All of the necessary files the switch needs are already in place on the switch. You do not need to (nor can you) create new files.
- The switch supports one SFTP session or one SCP session at a time.
- All files have read-write permission. Several SFTP commands, such as `create` or `remove`, are not allowed and return an error message. The switch displays the following files:

```
/
+---cfg
|   running-config
|   startup-config
+---log
|   crash-data
|   crash-data-a
|   crash-data-b
|   crash-data-c
|   crash-data-d 8212zl only
|   crash-data-e            "      "
|   crash-data-f  ""
|   crash-data-g  8212zl only
|   crash-data-h            "      "
|   crash-data-I  ""
|   crash-data-J  ""
|   crash-data-K  ""
|   crash-data-L  "    "
|   crash-log
|   crash-log-a
|   crash-log-b
|   crash-log-c
|   crash-log-d   8212zl only
|   crash-log-e  ""
|   crash-log-f  ""
|   crash-log-g  8212zl only
|   crash-log-h  " "
|   crash-log-I  " "
|   crash-log-J  " "
|   crash-log-K  " "
|   crash-log-L  " "
|   event log
+---os
|   primary
|   secondary
\---ssh
    +---mgr_keys
    |   authorized_keys
    \---oper_keys
    |   authorized_keys
\---core   (this directory is not available on the 8212zl)
|   mm1.cor      management module or management function
|   im_a.cor     interface module (chassis switches only)
|   im_b.cor     interface module (chassis switches only)
|   im_1.cor     interface module (chassis switches only)
|   port_1-24.cor         core-dump for ports 1-24 (stackable switches only)
|   port_25-48.cor        core-dump for ports 25-48 (stackable switches only)
```

- When using SFTP to copy a software image onto the switch, the command return takes only a few seconds. However, this does not mean that the transfer is complete, because the switch requires additional time (typically more than one minute) to write the image to flash in the background. To verify the file transfer has been completed, you can use the `show flash` command or look for a confirmation message in the log, as in the following example:

  ```
  I 01/09/09 16:17:07 00150 update: Primary Image updated.
  ```

Troubleshooting SSH, SFTP, and SCP operations

You can verify secure file transfer operations by checking the switch's event log, or by viewing the error messages sent by the switch that most SCP and SFTP clients print out on their console.

NOTE: Messages that are sent by the switch to the client depend on the client software in use to display them on the user console.

Broken SSH connection

If an ssh connection is broken at the wrong moment (for instance, the link goes away or spanning tree brings down the link), a fatal exception occurs on the switch. If this happens, the switch gracefully exits the session and produces an Event Log message indicating the cause of failure. The following three examples show the error messages that may appear in the log, depending on the type of session that is running (SSH, SCP, or SFTP):

```
ssh: read error Bad file number, session aborted I 01/01/90
00:06:11 00636 ssh: sftp session from ::ffff:10.0.12.35 W
01/01/90 00:06:26 00641 ssh:

sftp read error Bad file number, session aborted I 01/01/90
00:09:54 00637 ssh: scp session from ::ffff:10.0.12.35 W 01/
01/90

ssh: scp read error Bad file number, session aborted
```

NOTE: The `Bad file number` is from the system error value and may differ depending on the cause of the failure. In the third example, the device file to read was closed as the device read was about to occur.

Attempt to start a session during a flash write

If you attempt to start an SCP (or SFTP) session while a flash write is in progress, the switch does not allow the SCP or SFTP session to start. Depending on the client software in use, the following error message may appear on the client console:

```
Received disconnect from 10.0.12.31: 2: Flash access in
```

```
progress

lost connection
```

Failure to exit from a previous session

This next example shows the error message that may appear on the client console if a new SCP (or SFTP) session is started from a client before the previous client session has been closed (the switch requires approximately ten seconds to timeout the previous session):

```
Received disconnect from 10.0.12.31: 2: Wait for previous
session to complete

lost connection
```

Attempt to start a second session

The switch supports only one SFTP session or one SCP session at a time. If a second session is initiated (for example, an SFTP session is running and then an SCP session is attempted), the following error message may appear on the client console:

```
Received disconnect from 10.0.12.31: 2: Other SCP/SFTP
session running

lost connection
```

About using USB to transfer files to and from the switch

The switch's USB port (labeled as *Auxiliary Port*) allows the use of a USB flash drive for copying configuration files to and from the switch. Beginning with software release K_12_XX or later, `copy` commands that used either `tftp` or `xmodem` now include an additional option for `usb` as a source or destination for file transfers.

Operating rules and restrictions on USB usage are:

- Unformatted USB flash drives must first be formatted on a PC (Windows FAT format). For devices with multiple partitions, only the first partition is supported. Devices with secure partitions are not supported.
- If they already exist on the device, subdirectories are supported. When specifying a ***`filename`*** , you must enter either the individual file name (if at the root) or the full path name (for example, **/subdir/filename**).
- To view the contents of a USB flash drive, use the `dir` command. This lists all files and directories at the root. To view the contents of a directory, you must specify the subdirectory name (that is, `dir subdirectory`).
- The USB port supports connection to a single USB device. USB hubs to add more ports are not supported.

NOTE: Some USB flash drives may not be supported on your switch. Consult the latest *Release Notes* for information on supported devices.

Using PCM+ to update switch software

HP Switch Manager Plus includes a software update utility for updating on HP Switch switch products. For further information, see the *Getting Started Guide and the Administrator's Guide*, provided electronically with the application.

About transferring switch configurations

Using the CLI commands described in the section beginning with "TFTP: Copying a configuration file to a remote host (CLI)" (page 295), you can copy switch configurations to and from a switch, or copy a software image to configure or replace an ACL in the switch configuration.

NOTE: For greater security, you can perform all TFTP operations using SFTP, as described in the section "Using SCP and SFTP" (page 309).

You can also use the `include-credentials` command to save passwords, secret keys, and other security credentials in the running config file. For more information, see the section on "Saving Security Credentials in a Config File" in the *Access Security Guide* for your switch.

About transferring ACL command files

This section describes how to upload and execute a command file to the switch for configuring or replacing an ACL in the switch configuration. Such files should contain only access control entry (ACE) commands. For more on this general topic, including an example of an ACL command file created offline, see the section "Editing ACLs and Creating an ACL Offline" in the "Access Control Lists (ACLs)" chapter of the latest *Access Security Guide* for your switch.

About copying diagnostic data to a remote host, USB device, PC or UNIX workstation

You can use the CLI to copy the following types of switch data to a text file in a destination device:

Command output	Sends the output of a switch CLI command as a file on the destination device.
Event log	Copies the switch's Event Log into a file on the destination device.
Crash data	Software-specific data useful for determining the reason for a system crash.
Crash log	Processor-specific operating data useful for determining the reason for a system crash.
Flight data recorder (FDR) logs	Information that is "interesting" at the time of the crash, as well as when the switch is not performing correctly but has not crashed.

The destination device and copy method options are as follows (CLI keyword is in bold):

- Remote Host via `TFTP`.
- Physically connected USB flash drive via the switch's `USB` port.
- Serially connected PC or UNIX workstation via **Xmodem**.

Behavior of autorun when USB port is disabled

Software versions K.13.XX operation

When using software version K.13.58, if the USB port is disabled (`no usb-port` command), the USB autorun function does not work in the USB port until the USB port is enabled, the config file is saved, and the switch is rebooted. The 5-volt power to the USB port remains on, even after the USB port has been disabled.

For software versions after K.13.58, the 5-volt power applied to the USB port is synchronized with the enabling of the USB port, that is, when the USB port is enabled, the 5 volts are supplied; when the USB port is disabled, the 5 volts are not supplied. For previous software versions, the power was supplied continuously. The autorun function does not require a switch reboot, but the USB device must be inserted at least once after the port is enabled so the switch recognizes that the device is present. If the USB device is inserted, and then the USB port is enabled, the switch does not recognize that a USB device is present.

Software version K.14.XX operation

For software versions K.14.XX, the USB port can be disabled and enabled without affecting the autorun feature. When the USB port is enabled, the autorun feature activates if a USB device is already inserted in the USB port.

Power is synchronized with the enabling and disabling of USB ports as described above for K.13.59 and later software.

About using USB autorun

USB autorun helps ease the configuration of HP Switch switches by providing a way to auto-execute CLI commands from a USB flash drive. Using this solution, you can create a command file (also known as an `AutoRun` file), write it to a USB storage device, and then execute the file simply by inserting the USB device into the switch's 'Auxiliary Port.' The AutoRun file is executed automatically when autorun is enabled on the switch and can be designed for various purposes, such as to configure the switch, to update software, or to retrieve diagnostic logs for troubleshooting purposes.

The overall USB autorun solution requires the following components:

- An HP Switch switch that can securely use USB autorun to load authorized configurations and write reporting information. This requires software versions K.13.01, T.13.01 or greater.
- The network management application *HP Switch Manager Plus* (PCM+). PCM+ is required to create a valid AutoRun file and to view the results after the file has been executed on the switch.
- A non-proprietary USB flash drive.

NOTE: The ability to create a valid AutoRun file will be incorporated into an upcoming HP Switch Manager update; see the HP Switch Manager documentation for details. For guidelines on using the USB port for basic file copy capabilities, see "About using USB to transfer files to and from the switch" (page 314).

Security considerations

By default, the switch is unsecured when shipped (that is, USB autorun is enabled by default). However, as soon as an operator or manager password is configured, autorun is disabled and must be re-enabled at the configuration level of the CLI before it can be used. The requirement to use PCM+ to create a valid AutoRun file helps prevent a nonauthorized command file from being created and processed by the switch.

In terms of physical security, access to the switch's console port and USB port are equivalent. Keeping the switch in a locked wiring closet or other secure space helps to prevent unauthorized physical access. As additional precautions, you have the following configuration options via the CLI (see Configuring autorun on the switch (CLI) (page 307)):

- Disable autorun by setting an operator or manager password.
- Disable or re-enable the USB autorun function via the CLI.
- Enable autorun in secure mode to verify signatures in autorun command files and to decrypt encrypted command files.

Troubleshooting autorun operations

You can verify autorun operations by checking the following items:

USB auxiliary port LEDs

The following table shows LED indications on the Auxiliary Port that allow you to identify the different USB operation states.

Color	State	Meaning
Green	Slow blinking	Switch is processing USB AutoRun file.
Green	Solid	Switch has finished processing USB AutoRun file. This LED state indicates the AutoRun file was successfully executed and the report files were generated. You can review the report files on a USB-enabled computer for more details. Upon removal of the USB device, the LED turns OFF.

Color	State	Meaning
N/A	Off	Indicates one or more of the following: • No USB device has been inserted. • A USB device that cannot be recognized as a USB storage device has been inserted. • No AutoRun file can be found on the inserted USB device.. If the USB device has just been removed from the port, the switch executes any post commands.
Amber	Fast blinking	Processing Error. The AutoRun file stops processing when an error is encountered (for example, no more disk space is available on the USB device to write the result and report files). For more information on the error, remove the USB device and inspect its contents on a USB-enabled computer.

AutoRun status files.

The following files are generated during autorun operations and written to the USB flash drive:

- Report files (.xml file)—show which CLI commands have been run. The file name includes a serial number and datetime stamp to indicate when and on which device the AutoRun file was executed.
- Result files (.txt file)—contain the CLI output for each command that was run on the switch, allowing you to verify whether a command was executed successfully or not.

NOTE: PCM+ provides a mechanism to read these status files and capture the results of the commands executed. It also allows you to verify the report files for their authenticity and reject files that have not been signed (for details, see the HP Switch Manager documentation).

The status files do not include any records of post commands that may have been executed after the USB flash drive was removed from the switch.

Event log or syslog

For details on how to use the switch's Event Log or syslog for help in isolating autorun-related problems, see "Using the Event Log for troubleshooting switch problems" (page 414).

Autorun secure mode

You can use autorun secure mode to verify the authenticity of autorun command files. Secure-mode is configured using the `autorun secure-mode` command and can be enabled under both of the following conditions:

- An encryption-key has already been configured using the `autorun encryption key` command.
- A trusted certificate for verifying autorun command files has been copied to the switch using the
  `copy [ tftp | usb ] autorun-cert-file`
  command.

There is an additional security option to install a valid key-pair for signing the result files that are generated during autorun operations. You can generate the key-pair on the switch using the `crypto key generate autorun [`*`rsa`*`]` command.

NOTE: You can also install the key-pair from a tftp server or via the USB port using the
`copy [ tftp | usb ] autorun-key-file` *`ipaddr filename`*
command. The filename must contain the private key and the matching public key in a X509 certificate structure. Both the private key and the X509 certificate must be in PEM format.

Operating notes and restrictions

- Autorun is enabled by default, until passwords are set on the device.
- Secure-mode and encryption-key are disabled by default.
- To enable secure mode, both an encryption key and trusted certificate must be set.
- If secure-mode is enabled, the following conditions apply:
  - The encryption-key cannot be removed or unconfigured.
  - The key-pair cannot be removed.
- If secure mode is disabled, the key-pair can be removed using the `crypto key zeorize autorun` command.
- When installing the autorun certificate file and/or the other key files, the files must be in PEM format.

Autorun and configuring passwords

When an operator or manager password is configured on a switch, autorun is disabled automatically, and a message is displayed on the screen, as shown in the following example:

```
HP Switch# password manager
New password for manager: *****
Please retype new password for manager: *****
Autorun is disabled as operator/manager is configured.
```

After passwords are set, you can re-enable autorun as needed using the `autorun` command.

For more information on configuring passwords, see chapter "Username and Password Security" in the *Access Security Guide* for your switch.

B Monitoring and Analyzing Switch Operation

Command Summary

Table 30 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
N/A	Accesses status and counters menu	-	-	(page 323)
show system[chassislocate | information | power-supply | temperature | fans]	Displays general system information about the switch.	-	(page 323)	(page 325)
[no] task-monitor cpu	Allows you to enable or disable the collection of processor utilization data.	Disabled	(page 325)	-
show management	Accesses switch management address information.	-	(page 326)	(page 326)
show modules [details]	Displays additional component information for SSM adn Mini-GBICS.	-	(page 327)	(page 328)
[no] allow-v1-modules	Enables Compatibility Mode for interoperation of v2 zl and zl modules in the same chassis.	Enabled	(page 328)	-
show interfaces brief	Displays port status	-	(page 328)	(page 328)
show interfaces	Provides an overview of port activity for all ports on the switch.	-	(page 329)	(page 330)
janet show interfaces *port-list*	Provides traffic details for the ports you specify.	-	(page 329)	-
clear statistics[*port-list* | global]	Clears all counters and statistics without rebooting the switch.	-	(page 329)	-
show mac-address [vlan *vlan-id*] [*port-list*] [*mac-addr*]	Lists all learned MAC addresses and finds the port on which the switch learned a specific MAC address.	-	(page 331)	(page 331)
show spanning-tree	Lists the MSTP configuration, root data, and per-port data.	-	(page 333)	-
show ip igmp show ip igmp config show ip igmp *vlan-id* show ip igmp group *ip-addr* show ip igmp groups show ip igmp statistics	Displays the IGMP status on a per-VLAN basis.	-	(page 334)	-
show vlan show vlan *vlan-id*	Displays VLAN information.	-	(page 335)	-
mirror *session-#* [name *session-name*] port *port-#*	Configures a local mirroring session.	-	Step 2	-
[no] mirror 1 - 4 port *exit-port-#* [name *name-str*]	Configures a local mirroring session.	-	(page 338)	-

Table 30 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
[no]interface interface *port/trunk/mesh* | vlan *vid-#* monitor all in | out | both mirror *session* [session]... [no-tag-added]	Configures traffic-direction criteria to select traffic.	-	(page 338)	-
[no] monitor mac *mac-addr* src | dst | both mirror session	Configures MAC-based criteria to select traffic.	-	(page 339)	-
mirror endpoint ip *src-ip src-udp-port dst-ip exit-port* [truncation]	Configures a remote mirroring destination on a remote switch.	-	(page 339)	-
mirror *session* remote ip *src-ip src-udp-port dst-ip*	Configures a remote mirroring destination on a local swtich.	-	(page 339)	-
mirror *session* port *exit-port*	Configures a local mirroring destination on the local switch.	-	(page 340)	-
interface *port/trunk/mesh* monitor all [in | out | both] mirror *session* [no-tag-added] monitor ip access-group *acl-name* in mirror *session* () service-policy *mirror-policy-name* in	Configures monitored traffic.	-	(page 340)	-
vlan *vid-#* monitor all [in | out | both] mirror *session* monitor ip access-group *acl-name* in mirror *session* () service-policy *mirror-policy-name* in monitor mac *mac-addr* src | dest | both mirror	Configures monitored traffic.	-	(page 340)	-
show monitor [endpoint | *session-number* | name *session-name*]	Configures monitored traffic.	-	(page 341)	-
N/A	Configures local mirroring.	-	-	(page 341)

Table 30 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
mirror endpoint ip *src-ip-addr src-udp-port dst-ip-addr* port *exit-port*	Configures on a remote switch the exit port to use in a remote mirroring session.	-	(page 339)	-
mirror 1 - 4 [name *name-str*] remote ip *src-ip src-udp-port dst-ip* [truncation]	Configures the mirroring source on the local switch.	-	(page 345)	-
[no]interface *port/trunk/mesh* | vlan *vid-#* monitor all[in | out | both][mirror 1 - 4 | *name-str*][1 - 4 | *name-str* ...]	Configures traffic-direction criteria to select traffic.	-	(page 343)	-
class[ipv4 | ipv6 *classname*] [no] [seq-number] [match | ignore *ip-protocol source-address destination-address*] [precedence *precedence-value*] [tos *tos-value*] [ip-dscp *codepoint*] [vlan *vlan-id*] policy mirror *policy-name* [no] [*seq-number*] [class ipv4 | ipv6 *classname* action mirror *session*] [action mirror *session*]... [no] default-class action mirror *session* [no]interface [*port/trunk* | vlan *vid-#*] service-policy *mirror-policy-name* in	Configures a mirroring policy to select inbound traffic.	-	(page 344)	-
[no] monitor mac *mac-addr* src | dst | both mirror *session*	Configures the MAC-based criteria to select traffic.	-	(page 344)	-
mirror endpoint ip *src-ip src-udp-port dst-ip exit-port-#* no mirror endpoint ip *src-ip src-udp-port dst-ip*	Used on a destination switch, configures the remote endpoint of a mirroring session.	-	(page 345)	-
mirror 1 - 4 port *exit-port-#* [name *name-str*] no mirror 1- 4	Assigns the exit port to use for the specified mirroring session.	-	(page 345)	-
[no] mirror 1 - 4 [name *name-str*] remote ip *src-ip src-udp-port dst-ip* [truncation]	Used on the source switch, uniquely associates the mirrored traffic in the specified session with a remote destination switch.	-	(page 346)	-
[no] interface *port/trunk/mesh* monitor all[in | out | both] mirror 1 - 4 | *name-str* [[1 - 4 | *name-str*] [1 - 4 | *name-str*]] [no-tag-added]	Assigns a mirroring source to a previously configured mirroring session on a source switch by specifying the port, trunk, and/or mesh sources to use, the direction of traffic to mirror, and the session.	-	(page 347)	-
vlan *vid-#* monitor all[in | out | both][mirror 1 -	Assigns a monitored VLAN source to a previously	-	(page 348)	-

Table 30 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
4 | *name-str*][1 - 4 | *name-str* 1 - 4 | *name-str* 1 - 4 | *name-str*]	configured mirroring session on a source switch by specifying the VLAN ID, the direction of traffic to mirror, and the session.			
[no] monitor mac *mac-addr* src | dest | both mirror 1 - 4 | *name-str* [1 - 4 | *name-str*][1 - 4 | *name-str*][1 - 4 | *name-str*]	Configures a source and/or destination MAC address as criteria for selecting traffic in one or more mirroring sessions on the switch.	-	(page 349)	-
[no] class [ipv4 | ipv6 *classname*]	Defines the name of a traffic class and specifies whether a policy is to be applied to IPv4 or IPv6 packets.	-	(page 350)	-
[no] [*seq-number*] [match | ignore *ip-protocol* *source-address* *destination-address*] [ip-dscp *codepoint*] [precedence *precedence-value*] [tos *tos-value*] [vlan *vlan-id*]	-	-	(page 351)	-
[no] policy mirror *policy-name*	Defines the name of a mirroring policy and enters the policy configuration context.	-	(page 351)	-
[no] [*seq-number*] class [ipv4 | ipv6 *classname*] action mirror *session*	Defines the mirroring action to be applied on a pre-configured IPv4 or IPv6 traffic class when a packet matches the match criteria in the traffic class.	-	(page 351)	-
[no] default-class action mirror *session* [action mirror *session*]...	Configures a default class that allows packets that are not matched nor ignored by any of the class configurations in a mirroring policy to be mirrored to the destination configured for the specified session.	-	(page 351)	-
interface *port-list* service-policy *policy-name* in	Configures the specified ports with a mirroring policy that is applied to inbound traffic on each interface.	-	(page 352)	-
vlan *vlan-id* service-policy *policy-name* in	Configures a mirroring policy on the specified VLAN that is applied to inbound traffic on the VLAN interface.	-	(page 352)	-
show monitor	Displays information on the currently configured status, traffic-selection criteria, and number of monitored interfaces in each mirroring session on a switch.	-	(page 352)	-

Table 30 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`show monitor endpoint`	Displays the remote mirroring endpoints configured on the switch.	-	(page 354)	-
`show monitor [ 1 - 4 | name` *`name-str`* `]`	Displays detailed configuration information for a specified local or remote mirroring session on a source switch.	-	(page 355)	-

Status and counters data

This section describes the status and counters screens available through the switch console interface and/or the WebAgent.

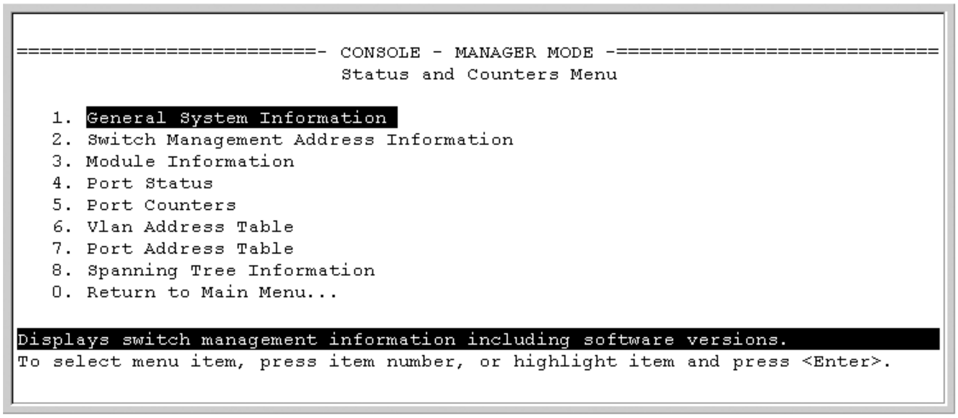
NOTE: You can access all console screens from the WebAgent via Telnet to the console. Telnet access to the switch is available in the **Device View** window under the **Configuration** tab.

Accessing status and counters (Menu)

Beginning at the Main Menu, display the Status and Counters menu by selecting:

1. Status and Counters

Figure 157 The Status and Counters menu



```
==========================- CONSOLE - MANAGER MODE -============================
                          Status and Counters Menu

   1. General System Information
   2. Switch Management Address Information
   3. Module Information
   4. Port Status
   5. Port Counters
   6. Vlan Address Table
   7. Port Address Table
   8. Spanning Tree Information
   0. Return to Main Menu...

Displays switch management information including software versions.
To select menu item, press item number, or highlight item and press <Enter>.
```

Each of the above menu items accesses the read-only screens described on the following pages. See the online help for a description of the entries displayed in these screens.

Accessing system information (CLI)

Syntax:

`show system [ chassislocate | information | power-supply | temperature | fans ]`

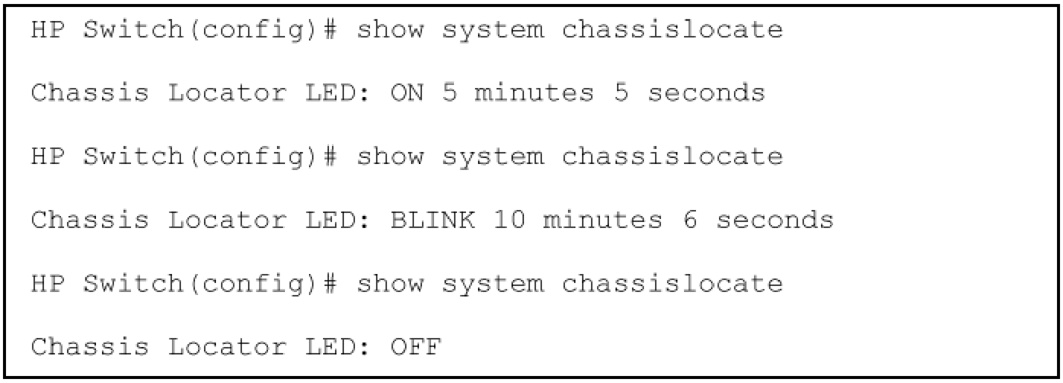
Displays global system information and operational parameters for the switch.

`chassislocate`	Displays the chassisLocator LED status. Possible values are ON, Off, or Blink. When the status is On or Blink, the number of minutes that the Locator LED will continue to be on or to blink is displayed. (See figure Figure 158 (page 324))
`information`	Displays global system information and operational parameters for the switch. (See Figure 160 (page 324).)

`power-supply`	Shows chassis power supply and settings.
`temperature`	Shows system temperature and settings.
`fans`	Shows system fan status. (See Figure 159 (page 324).)

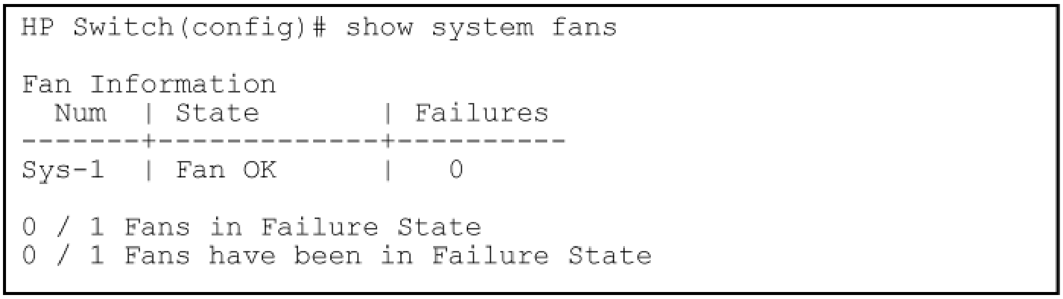
Example

Figure 158 Command results for `show system chassislocate` command



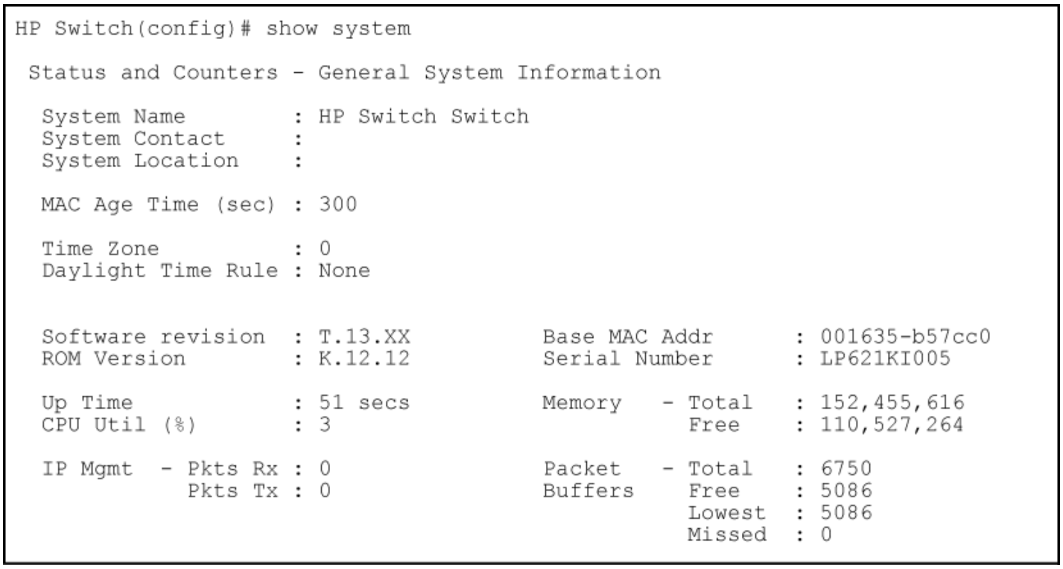
```
HP Switch(config)# show system chassislocate

Chassis Locator LED: ON 5 minutes 5 seconds

HP Switch(config)# show system chassislocate

Chassis Locator LED: BLINK 10 minutes 6 seconds

HP Switch(config)# show system chassislocate

Chassis Locator LED: OFF
```

Figure 159 System fan status



```
HP Switch(config)# show system fans

Fan Information
  Num  | State       | Failures
-------+-------------+----------
Sys-1  | Fan OK      |   0

0 / 1 Fans in Failure State
0 / 1 Fans have been in Failure State
```

Figure 160 Switch system information



```
HP Switch(config)# show system

 Status and Counters - General System Information

  System Name        : HP Switch Switch
  System Contact     :
  System Location    :

  MAC Age Time (sec) : 300

  Time Zone          : 0
  Daylight Time Rule : None


  Software revision  : T.13.XX          Base MAC Addr      : 001635-b57cc0
  ROM Version        : K.12.12          Serial Number      : LP621KI005

  Up Time            : 51 secs          Memory    - Total    : 152,455,616
  CPU Util (%)       : 3                            Free     : 110,527,264

  IP Mgmt   - Pkts Rx : 0                Packet    - Total    : 6750
               Pkts Tx : 0                Buffers     Free     : 5086
                                                    Lowest   : 5086
                                                    Missed   : 0
```

Collecting processor data with the task monitor (CLI)

The task monitor feature allows you to enable or disable the collection of processor utilization data. The `task-monitor cpu` command is equivalent to the existing debug mode command `taskusage -d`. (The `taskUsageShow` command is also available.)

When the `task-monitor` command is enabled, the `show cpu` command summarizes the processor usage by protocol and system functions.

Syntax:

`[ no ] task-monitor cpu`

Allows the collection of processor utilization data.

Only manager logins can execute this command.

The settings are not persistent, that is, there are no changes to the configuration.

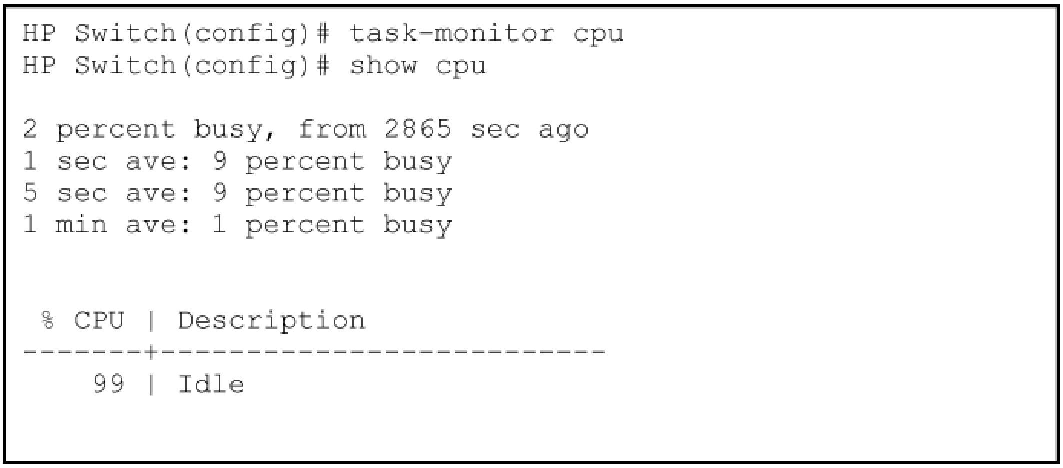
(Default: Disabled)

The task monitor feature allows you to enable or disable the collection of processor utilization data. The `task-monitor cpu` command is equivalent to the existing debug mode command `taskusage -d`. (The `taskUsageShow` command is available as well.)

When the `task-monitor` command is enabled, the `show cpu` command summarizes the processor usage by protocol and system functions.

Example

Figure 161 The `task-monitor cpu` command and `show cpu` output



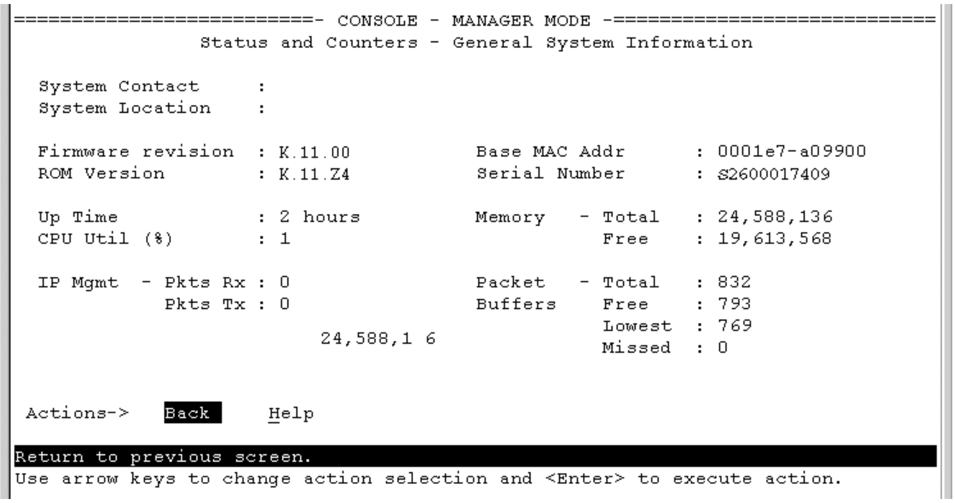
```
HP Switch(config)# task-monitor cpu
HP Switch(config)# show cpu

2 percent busy, from 2865 sec ago
1 sec ave: 9 percent busy
5 sec ave: 9 percent busy
1 min ave: 1 percent busy


 % CPU | Description
-------+-------------------------
    99 | Idle
```

Accessing system information (Menu)

From the console Main Menu, select:

1. Status and Counters
1. General System Information

Figure 162 Example of general switch information



```
==========================- CONSOLE - MANAGER MODE -============================
                Status and Counters - General System Information

  System Contact      :
  System Location     :

  Firmware revision   : K.11.00          Base MAC Addr      : 0001e7-a09900
  ROM Version         : K.11.Z4          Serial Number      : S2600017409

  Up Time             : 2 hours          Memory    - Total  : 24,588,136
  CPU Util (%)        : 1                            Free   : 19,613,568

  IP Mgmt   - Pkts Rx : 0                Packet    - Total  : 832
              Pkts Tx : 0                Buffers     Free   : 793
                                                     Lowest : 769
                          24,588,1 6                 Missed : 0


 Actions->   Back     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

This screen dynamically indicates how individual switch resources are being used. See the online Help for details.

Accessing switch management address information (CLI)

Syntax:

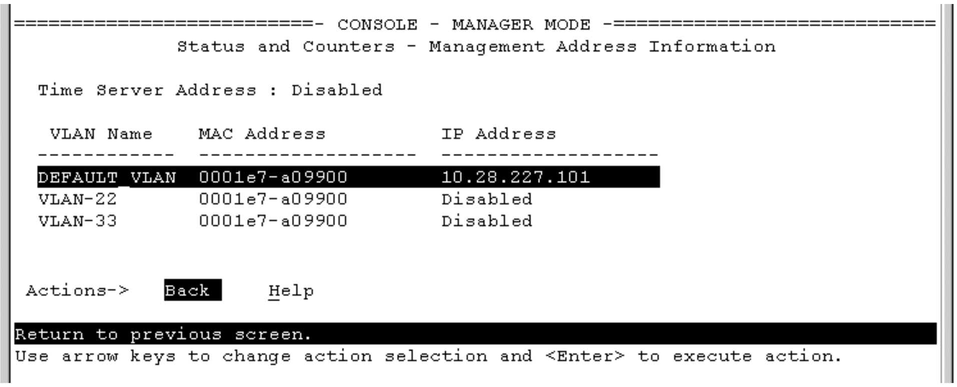
```
show management
```

Accessing switch management address information (Menu)

From the Main Menu, select:

1. **Status and Counters ...**
2. **Switch Management Address Information**

Figure 163 Example of management address information with VLANs configured



```
==========================- CONSOLE - MANAGER MODE -============================
              Status and Counters - Management Address Information

  Time Server Address : Disabled

   VLAN Name     MAC Address          IP Address
  ------------  -------------------  -------------------
  DEFAULT_VLAN  0001e7-a09900        10.28.227.101
  VLAN-22       0001e7-a09900        Disabled
  VLAN-33       0001e7-a09900        Disabled


 Actions->   Back     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

This screen displays addresses that are important for management of the switch. If multiple VLANs are *not configured*, this screen displays a single IP address for the entire switch. See the online Help for details.

NOTE: As shown in Figure 163 (page 326), all VLANs on the switches use the same **MAC address**. (This includes both the statically configured VLANs and any dynamic VLANs existing on the switch as a result of GVRP operation.)

Also, the switches use a multiple forwarding database. When using multiple VLANs and connecting a switch to a device that uses a single forwarding database, such as a Switch 4000M, there are cabling and tagged port VLAN requirements. For more information on this topic, see "Multiple VLAN Considerations" in the "Static Virtual LANs (VLANs)" chapter of the *Advanced Traffic Management Guide* for your switch.

Viewing additional component information (CLI)

The CLI `show modules` command displays additional component information for the following:

- SSM—identification, including serial number
- Mini-GBICS—a list of installed mini-GBICs displaying the type, "J" number, and serial number (when available)

Syntax:

`show modules [details]`

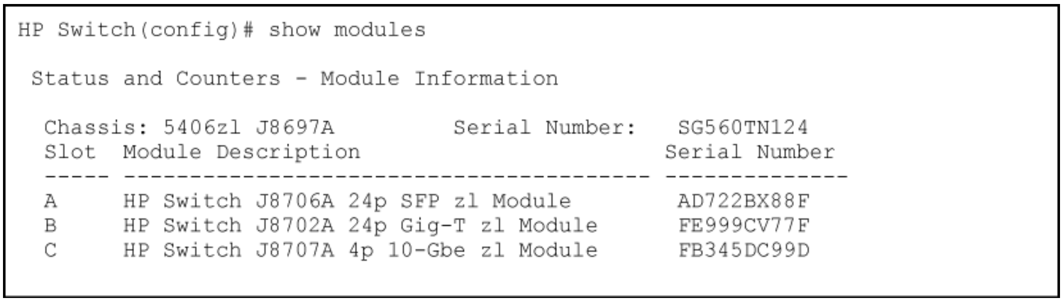
Displays information about the installed modules (Figure 164 (page 327)), including:

- The slot in which the module is installed
- The module description
- The serial number
- The SSM description, serial number, and status (8200zl switches only)

Additionally, this command displays the part number (J number) and serial number of the chassis. (See Figure 165 (page 327).)

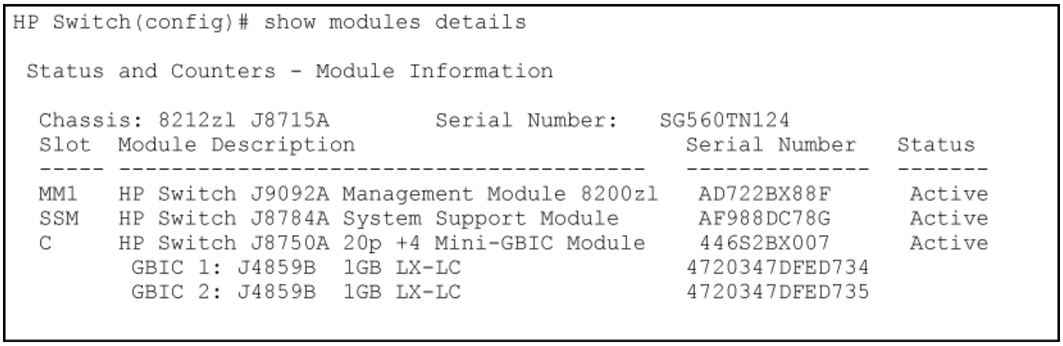
Examples

Figure 164 The `show modules` command output



```
HP Switch(config)# show modules

 Status and Counters - Module Information

  Chassis: 5406zl J8697A         Serial Number:   SG560TN124
  Slot  Module Description                       Serial Number
  ----- ---------------------------------------- --------------
  A     HP Switch J8706A 24p SFP zl Module        AD722BX88F
  B     HP Switch J8702A 24p Gig-T zl Module      FE999CV77F
  C     HP Switch J8707A 4p 10-Gbe zl Module      FB345DC99D
```

Figure 165 The `show modules details` command for the 8212zl, showing SSM and mini-GBIC information



```
HP Switch(config)# show modules details

 Status and Counters - Module Information

  Chassis: 8212zl J8715A        Serial Number:   SG560TN124
  Slot  Module Description                         Serial Number   Status
  ----- ----------------------------------------   --------------  -------
  MM1   HP Switch J9092A Management Module 8200zl   AD722BX88F      Active
  SSM   HP Switch J8784A System Support Module      AF988DC78G      Active
  C     HP Switch J8750A 20p +4 Mini-GBIC Module    446S2BX007      Active
         GBIC 1: J4859B  1GB LX-LC                 4720347DFED734
         GBIC 2: J4859B  1GB LX-LC                 4720347DFED735
```

NOTE: On HP Switch 3500yl and 6200yl series switches, the mini-GBIC information does not display, because the ports are fixed and not part of any module.

Viewing port status (Menu)

From the Main Menu, select:

1. Status and Counters ...
3. Module Information

Enabling and Disabling Compatibility Mode for v2 zl and zl modules

NOTE: In the following context, v2 zl modules are the second version of the current zl modules. Both v2 zl and zl modules are supported in the 5400zl and 8200zl series chassis switches.

Compatibility Mode allows the inter-operation of v2 zl modules with zl modules in a chassis switch. When in Compatibility Mode, the switch accepts either v2 zl or zl modules. The default is Compatibility Mode enabled. If Compatibility Mode is disabled by executing the `no allow-v1-modules` command, the switch will only power up v2 zl modules.

Syntax:

```
[ no ] allow-v1-modules
```

Enables Compatibility Mode for interoperation of v2 zl and zl modules in the same chassis. (See Figure 166 (page 328).)

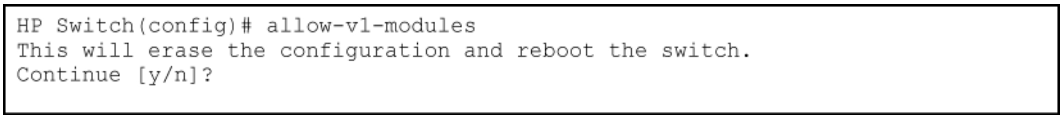
The `no` form of the command disables Compatibility Mode. Only the v2 zl modules are powered up. (See Figure 167 (page 328).)

(Default: Enabled.)

For information about how the switch modules behave in various situations and combinations, see "Compatibility mode" (page 361).

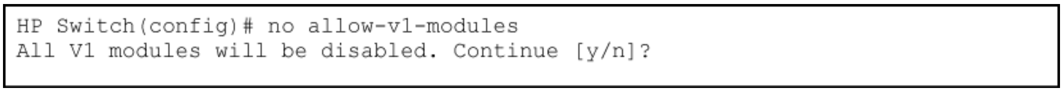
Examples

Figure 166 Enabling compatibility mode



```
HP Switch(config)# allow-v1-modules
This will erase the configuration and reboot the switch.
Continue [y/n]?
```

Figure 167 Disabling compatibility mode



```
HP Switch(config)# no allow-v1-modules
All V1 modules will be disabled. Continue [y/n]?
```

Viewing port status (CLI)

Syntax:

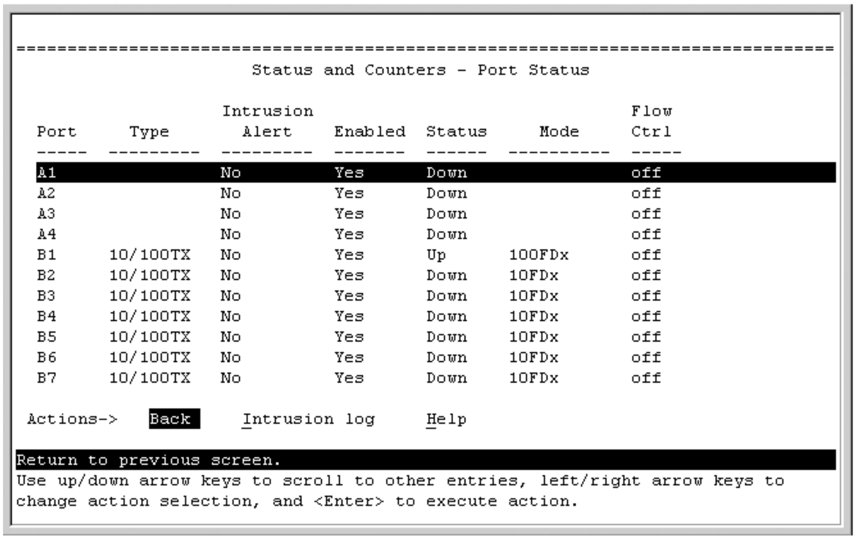
```
show interfaces brief
```

Viewing port status (Menu)

From the Main Menu, select:

1. Status and Counters ...
4. Port Status

Figure 168 Example of port status on the menu interface



```
===============================================================================
                       Status and Counters - Port Status

                   Intrusion                                     Flow
  Port     Type      Alert     Enabled  Status      Mode         Ctrl
  -----  ---------  ---------  -------  ------   ----------      -----
  A1                No         Yes      Down                     off
  A2                No         Yes      Down                     off
  A3                No         Yes      Down                     off
  A4                No         Yes      Down                     off
  B1     10/100TX   No         Yes      Up       100FDx          off
  B2     10/100TX   No         Yes      Down     10FDx           off
  B3     10/100TX   No         Yes      Down     10FDx           off
  B4     10/100TX   No         Yes      Down     10FDx           off
  B5     10/100TX   No         Yes      Down     10FDx           off
  B6     10/100TX   No         Yes      Down     10FDx           off
  B7     10/100TX   No         Yes      Down     10FDx           off

 Actions->   Back     Intrusion log     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

Accessing port and trunk group statistics (CLI)

Viewing the port counter summary report

Syntax:

`show interfaces`

Provides an overview of port activity for all ports on the switch.

Viewing a detailed traffic summary for specific ports

Syntax:

`show interfaces` *`port-list`*

Provides traffic details for the ports you specify.

Resetting the port counters

It is useful to be able to clear all counters and statistics without rebooting the switch when troubleshooting network issues. The `clear statistics global` command clears all counters and statistics for all interfaces except SNMP. You can also clear the counters and statistics for an individual port using the `clear statistics` *`port-list`* command.

Syntax:

`clear statistics [` *`port-list`* `| global ]`

When executed with the *`port-list`* option, clears the counters and statistics for an individual port.

When executed with the `global` option, clears all counters and statistics for all interfaces except SNMP.

The `show interfaces [`*`port-list`*`]` command displays the totals accumulated since the last boot or the last `clear statistics` command was executed. The menu page also displays these totals.

SNMP displays the counter and statistics totals accumulated since the last reboot; it is not affected by the `clear statistics global` command or the `clear statistics` *`port-list`* command. An SNMP trap is sent whenever the statistics are cleared.

Viewing port and trunk group statistics (WebAgent)

1. In the navigation pane of the WebAgent, click Interface.
2. Click Port Info/Config.

For information about this screen, click **?** in the upper right corner of the WebAgent screen.

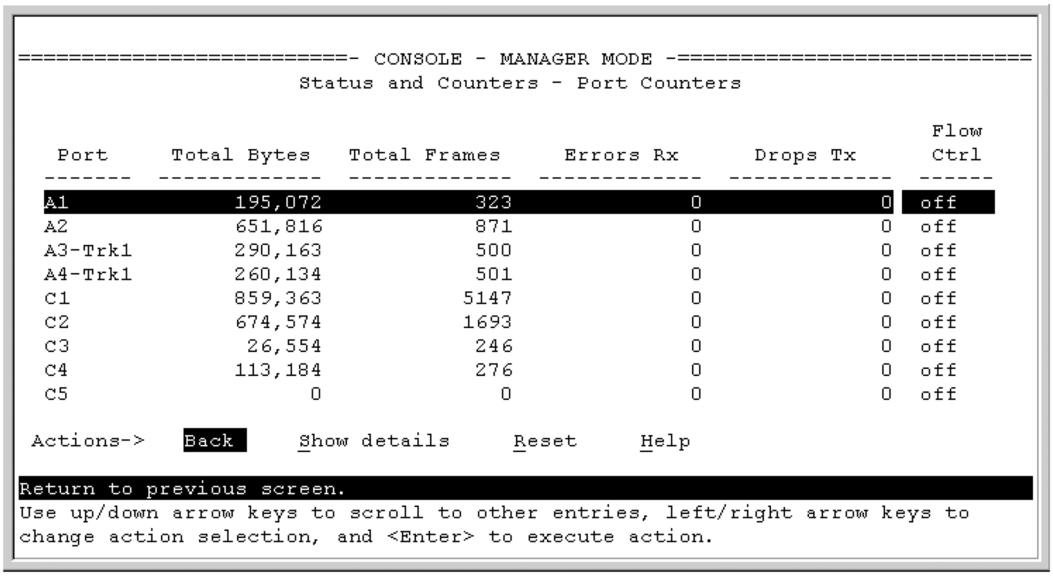
NOTE: to reset the port counters to zero, you must reboot the switch.

Accessing port and trunk statistics (Menu)

From the Main Menu, select:

1. Status and Counters ...
4. Port Counters

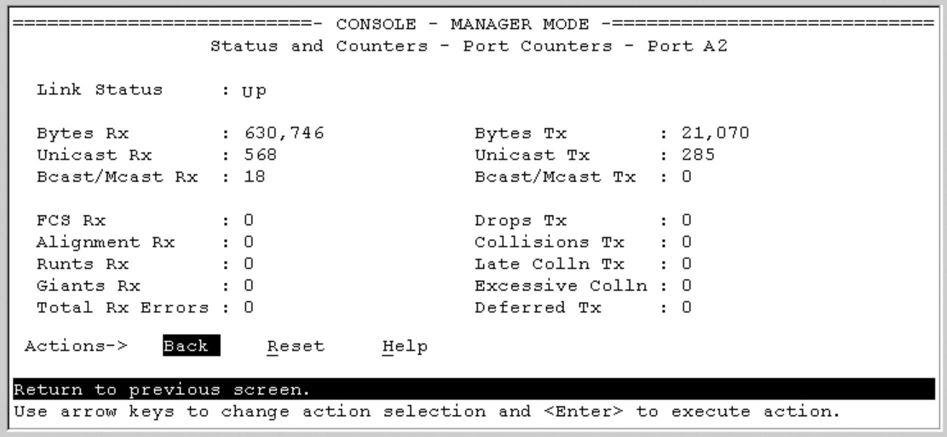
Figure 169 Example of port counters on the menu interface



```
=========================- CONSOLE - MANAGER MODE -===========================
                      Status and Counters - Port Counters

                                                                      Flow
  Port      Total Bytes   Total Frames    Errors Rx      Drops Tx     Ctrl
 -------   -------------  -------------  -------------  -------------  ------
 A1             195,072            323              0              0  off
 A2             651,816            871              0              0  off
 A3-Trk1        290,163            500              0              0  off
 A4-Trk1        260,134            501              0              0  off
 C1             859,363           5147              0              0  off
 C2             674,574           1693              0              0  off
 C3              26,554            246              0              0  off
 C4             113,184            276              0              0  off
 C5                   0              0              0              0  off

 Actions->   Back     Show details     Reset     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

To view details about the traffic on a particular port, use the ↓ key to highlight that port number, then select **Show Details**. For example, selecting port A2 displays a screen similar to Figure 170 (page 330), below.

Figure 170 Example of the display for `Show Details` on a selected port



```
=========================- CONSOLE - MANAGER MODE -===========================
                 Status and Counters - Port Counters - Port A2

  Link Status     : Up

  Bytes Rx        : 630,746             Bytes Tx        : 21,070
  Unicast Rx      : 568                 Unicast Tx      : 285
  Bcast/Mcast Rx  : 18                  Bcast/Mcast Tx  : 0

  FCS Rx          : 0                   Drops Tx        : 0
  Alignment Rx    : 0                   Collisions Tx   : 0
  Runts Rx        : 0                   Late Colln Tx   : 0
  Giants Rx       : 0                   Excessive Colln : 0
  Total Rx Errors : 0                   Deferred Tx     : 0

 Actions->   Back     Reset     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

This screen also includes the **Reset** action for the current session. (See the "NOTE" (page 362).)

Notes:

Once cleared, statistics cannot be reintroduced.

Viewing the switch's MAC address tables

Accessing MAC address views and searches (CLI)

Syntax:

```
show mac-address
[vlan vlan-id ]
[ port-list ]
[ mac-addr ]
```

Listing all learned MAC addresses on the switch, with the port number on which each MAC address was learned

```
HP Switch# show mac-address
```

Listing all learned MAC addresses on one or more ports, with their corresponding port numbers

For example, to list the learned MAC address on ports A1 through A4 and port A6:

```
HP Switch# show mac-address a1-a4,a6
```

Listing all learned MAC addresses on a VLAN, with their port numbers

This command lists the MAC addresses associated with the ports for a given VLAN. For example:

```
HP Switch# show mac-address vlan 100
```

NOTE: The switches operate with a multiple forwarding database architecture.

Finding the port on which the switch learned a specific MAC address

For example, to find the port on which the switch learns a MAC address of 080009-21ae84:

```
Select VLAN : DEFAULT_VLAN
```

Accessing MAC address views and searches (Menu)

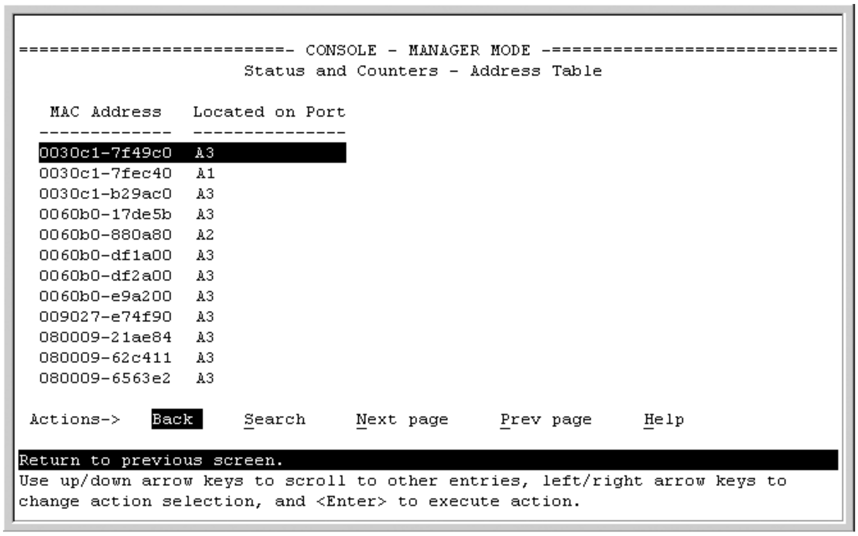
Viewing and searching per-VLAN MAC-addresses

This feature lets you determine which switch port on a selected VLAN is being used to communicate with a specific device on the network.

From the Main Menu, select:

1. Status and Counters ...
5. VLAN Address Table

1. The switch then prompts you to select a VLAN.

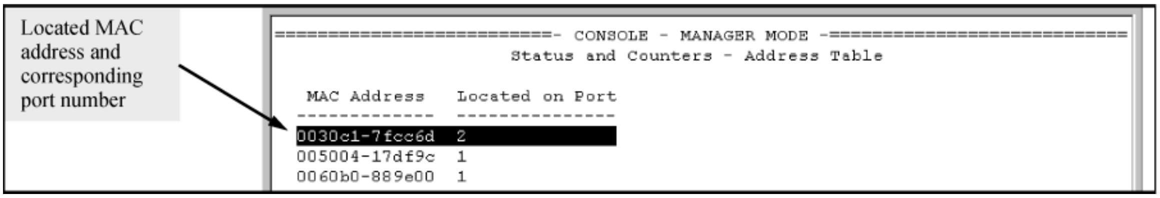


```
==========================- CONSOLE - MANAGER MODE -============================
                        Status and Counters - Address Table

   MAC Address    Located on Port
  -------------  ---------------
  0030c1-7f49c0   A3
  0030c1-7fec40   A1
  0030c1-b29ac0   A3
  0060b0-17de5b   A3
  0060b0-880a80   A2
  0060b0-df1a00   A3
  0060b0-df2a00   A3
  0060b0-e9a200   A3
  009027-e74f90   A3
  080009-21ae84   A3
  080009-62c411   A3
  080009-6563e2   A3

 Actions->    Back     Search     Next page     Prev page     Help

Return to previous screen.
Use up/down arrow keys to scroll to other entries, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

2. Use the Space bar to select the VLAN you want, and then press **[Enter]**.

   The switch then displays the MAC address table for that VLAN (Figure 171 (page 332)).

Figure 171 Example of the address table



Located MAC address and corresponding port number

```
==========================- CONSOLE - MANAGER MODE -============================
                        Status and Counters - Address Table

   MAC Address    Located on Port
  -------------  ---------------
  0030c1-7fcc6d   2
  005004-17df9c   1
  0060b0-889e00   1
```

To page through the listing, use **Next page** and **Prev page**.

Finding the port connection for a specific device on a VLAN

This feature uses a device's MAC address that you enter to identify the port used by that device.

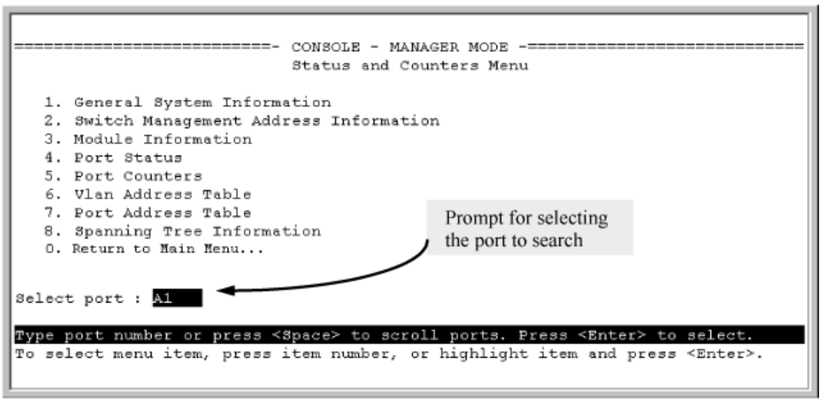
1. Proceeding from Figure 171 (page 332), press **[S]** (for **Search**), to display the following prompt:

```
Enter MAC address: _
```

2. Enter the MAC address you want to locate and press **[Enter]**.

   The address and port number are highlighted if found (Figure 172 (page 332)). If the switch does not find the MAC address on the currently selected VLAN, it leaves the MAC address listing empty.

Figure 172 Example of menu indicating located MAC address



Prompt for selecting the port to search

```
==========================- CONSOLE - MANAGER MODE -============================
                           Status and Counters Menu

   1. General System Information
   2. Switch Management Address Information
   3. Module Information
   4. Port Status
   5. Port Counters
   6. Vlan Address Table
   7. Port Address Table
   8. Spanning Tree Information
   0. Return to Main Menu...


Select port : A1

Type port number or press <Space> to scroll ports. Press <Enter> to select.
To select menu item, press item number, or highlight item and press <Enter>.
```

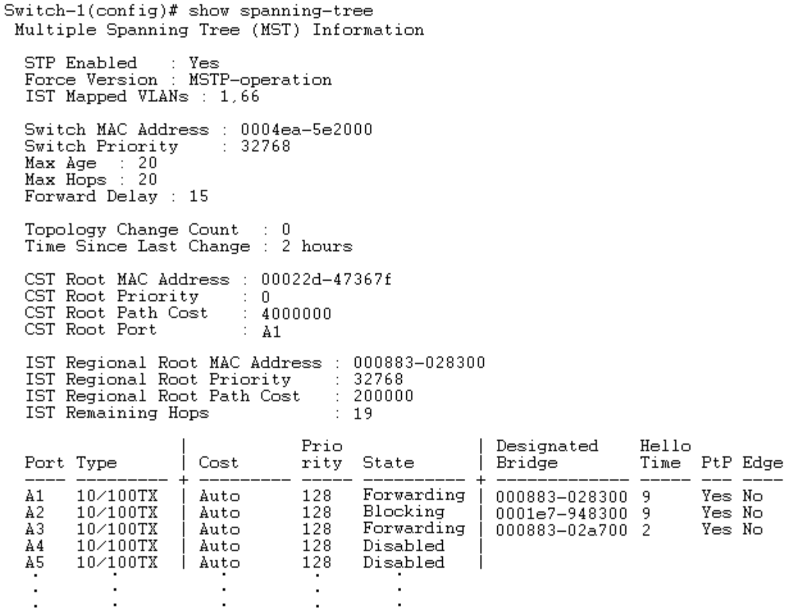
3. Press **[P]** (for **Prev page**) to return to the full address table listing.

Viewing and searching port-level MAC addresses

This feature displays and searches for MAC addresses on the specified port instead of for all ports on the switch.

1. From the Main Menu, select:
   1. Status and Counters ...
   7. Port Address Table

   Figure 173 Listing MAC addresses for a specific port

```
Switch-1(config)# show spanning-tree
 Multiple Spanning Tree (MST) Information

  STP Enabled   : Yes
  Force Version : MSTP-operation
  IST Mapped VLANs : 1,66

  Switch MAC Address : 0004ea-5e2000
  Switch Priority    : 32768
  Max Age  : 20
  Max Hops : 20
  Forward Delay : 15

  Topology Change Count  : 0
  Time Since Last Change : 2 hours

  CST Root MAC Address : 00022d-47367f
  CST Root Priority    : 0
  CST Root Path Cost   : 4000000
  CST Root Port        : A1

  IST Regional Root MAC Address : 000883-028300
  IST Regional Root Priority    : 32768
  IST Regional Root Path Cost   : 200000
  IST Remaining Hops            : 19

                 |           Prio             | Designated    Hello
  Port Type      | Cost      rity  State      | Bridge        Time  PtP Edge
  ---- --------- + --------- ----- ---------- + ------------- ----- --- ----
  A1   10/100TX  | Auto      128   Forwarding | 000883-028300 9     Yes No
  A2   10/100TX  | Auto      128   Blocking   | 0001e7-948300 9     Yes No
  A3   10/100TX  | Auto      128   Forwarding | 000883-02a700 2     Yes No
  A4   10/100TX  | Auto      128   Disabled   |
  A5   10/100TX  | Auto      128   Disabled   |
   .       .         .        .       .
   .       .         .        .       .
   .       .         .        .       .
```

2. Use the Space bar to select the port you want to list or search for MAC addresses, then press **[Enter]** to list the MAC addresses detected on that port.

Determining whether a specific device is connected to the selected port

Proceeding from step 2 (page 333), above:

1. Press **[S]** (for **Search**), to display the following prompt:

   ```
   Enter MAC address: _
   ```

2. Enter the MAC address you want to locate and press **[Enter]**.

   The address is highlighted if found. If the switch does not find the address, it leaves the MAC address listing empty.

3. Press **[P]** (for **Prev page**) to return to the previous per-port listing.

Accessing MSTP Data (CLI)

Syntax:

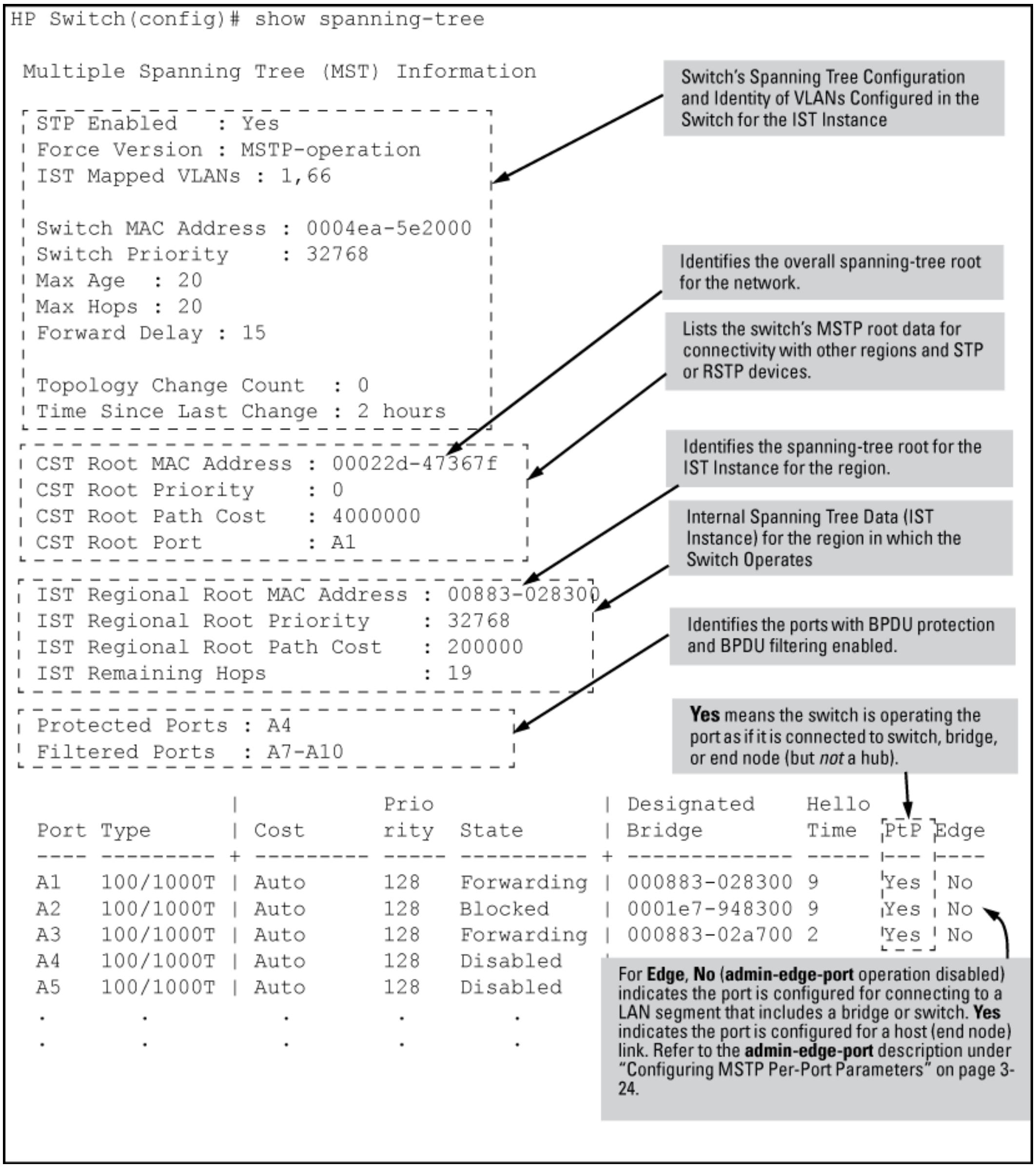
```
show spanning-tree
```

Displays the switch's global and regional spanning-tree status, plus the per-port spanning-tree operation at the regional level.

Values for the following parameters appear only for ports connected to active devices: `Designated Bridge`, `Hello Time`, `PtP`, and `Edge`.

Example

Figure 174 Output from `show spanning-tree` command



```
HP Switch(config)# show spanning-tree

 Multiple Spanning Tree (MST) Information

  STP Enabled    : Yes
  Force Version : MSTP-operation
  IST Mapped VLANs : 1,66

  Switch MAC Address : 0004ea-5e2000
  Switch Priority     : 32768
  Max Age   : 20
  Max Hops : 20
  Forward Delay : 15

  Topology Change Count   : 0
  Time Since Last Change : 2 hours

  CST Root MAC Address : 00022d-47367f
  CST Root Priority     : 0
  CST Root Path Cost    : 4000000
  CST Root Port         : A1

  IST Regional Root MAC Address : 00883-028300
  IST Regional Root Priority     : 32768
  IST Regional Root Path Cost    : 200000
  IST Remaining Hops             : 19

  Protected Ports : A4
  Filtered Ports   : A7-A10

                   |          Prio              | Designated     Hello
  Port Type        | Cost     rity  State       | Bridge         Time  PtP Edge
  ---- ---------   + --------- ----- ---------- + -------------  ----- --- ----
  A1   100/1000T  | Auto      128   Forwarding | 000883-028300 9     Yes  No
  A2   100/1000T  | Auto      128   Blocked    | 0001e7-948300 9     Yes  No
  A3   100/1000T  | Auto      128   Forwarding | 000883-02a700 2     Yes  No
  A4   100/1000T  | Auto      128   Disabled
  A5   100/1000T  | Auto      128   Disabled
  .    .            .         .     .
  .    .            .         .     .
```

Switch's Spanning Tree Configuration and Identity of VLANs Configured in the Switch for the IST Instance

Identifies the overall spanning-tree root for the network.

Lists the switch's MSTP root data for connectivity with other regions and STP or RSTP devices.

Identifies the spanning-tree root for the IST Instance for the region.

Internal Spanning Tree Data (IST Instance) for the region in which the Switch Operates

Identifies the ports with BPDU protection and BPDU filtering enabled.

Yes means the switch is operating the port as if it is connected to switch, bridge, or end node (but *not* a hub).

For **Edge**, **No** (**admin-edge-port** operation disabled) indicates the port is configured for connecting to a LAN segment that includes a bridge or switch. **Yes** indicates the port is configured for a host (end node) link. Refer to the **admin-edge-port** description under "Configuring MSTP Per-Port Parameters" on page 3-24.

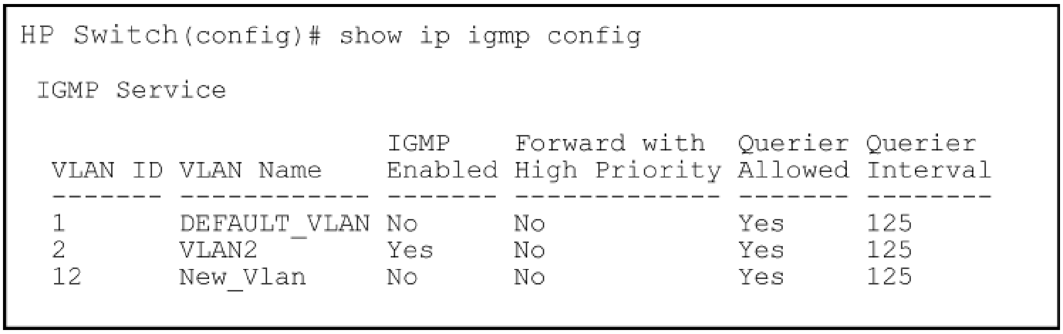
Viewing internet IGMP status (CLI)

Show command	Output
`show ip igmp`	Global command listing IGMP status for all VLANs configured in the switch: • VLAN ID (VID) and name • Querier address • Active group addresses per VLAN • Number of report and query packets per group • Querier access port per VLAN
`show ip igmp config`	Displays the IGMP configuration information, including VLAN ID, VLAN name, status, forwarding, and Querier information.
`show ip igmp` *`vlan-id`*	Per-VLAN command listing above, IGMP status for specified VLAN (VID)

Show command	Output
`show ip igmp group ip-addr`	Lists the ports currently participating in the specified group, with port type, Access type, Age Timer data and Leave Timer data.
`show ip igmp groups`	Displays VLAN-ID, group address, uptime, expiration time, multicast filter type, and the last reporter for IGMP groups.
`show ip igmp statistics`	Displays IGMP operational information, such as VLAN IDs and names, and filtered and flooding statistics.

Examples

Example 61 Output from `show ip igmp config` command



```
HP Switch(config)# show ip igmp config

 IGMP Service

                         IGMP    Forward with  Querier Querier
  VLAN ID VLAN Name      Enabled High Priority Allowed Interval
  ------- ------------   ------- ------------- ------- --------
  1       DEFAULT_VLAN   No      No            Yes     125
  2       VLAN2          Yes     No            Yes     125
  12      New_Vlan       No      No            Yes     125
```

Example 62 IGMP statistical information

```
HP Switch(vlan-2)# show ip igmp statistics

 IGMP Service Statistics

  Total VLANs with IGMP enabled               : 1
  Current count of multicast groups joined    : 1


 IGMP Joined Groups Statistics

  VLAN ID VLAN Name                        Filtered     Flood
  ------- -------------------------------- ------------ ------------

  2       VLAN2                            2            1
```

Viewing VLAN information (CLI)

Show command	Output
`show vlan`	Lists: • Maximum number of VLANs to support • Existing VLANs • Status (static or dynamic) • Primary VLAN
`show vlan vlan-id`	For the specified VLAN, lists: • Name, VID, and status (static/dynamic) • Per-port mode (tagged, untagged, forbid, no/auto)

Show command	Output
	• "Unknown VLAN" setting (Learn, Block, Disable) • Port status (up/down)

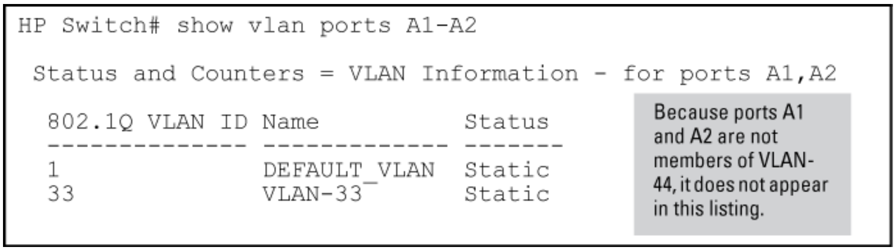
Example

Suppose that your switch has the following VLANs:

Ports	VLAN	VID
A1-A12	DEFAULT_VLAN	1
A1, A2	VLAN-33	33
A3, A4	VLAN-44	44

The next three figures show how you could list data on the above VLANs.

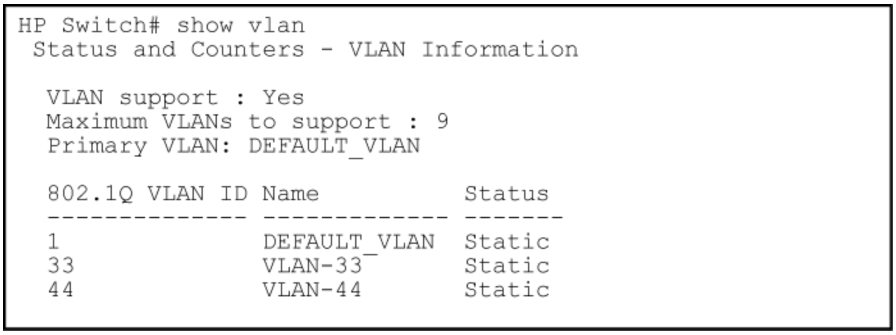
Figure 175 Listing the VLAN ID (vid) and status for specific ports



```
HP Switch# show vlan ports A1-A2

 Status and Counters = VLAN Information - for ports A1,A2

  802.1Q VLAN ID Name          Status
  -------------- ------------- -------
  1              DEFAULT_VLAN  Static
  33             VLAN-33       Static
```

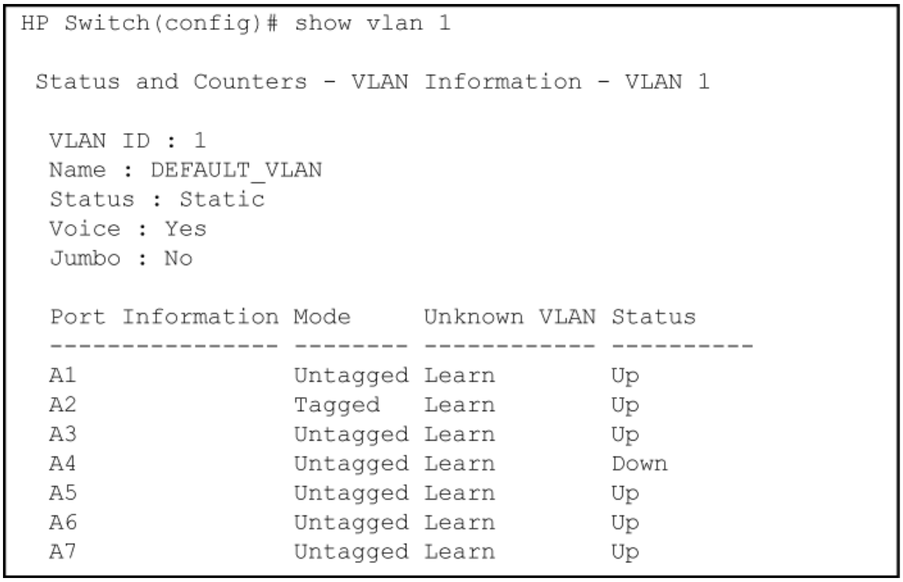
Because ports A1 and A2 are not members of VLAN-44, it does not appear in this listing.

Figure 176 Example of VLAN listing for the entire switch



```
HP Switch# show vlan
 Status and Counters - VLAN Information

  VLAN support : Yes
  Maximum VLANs to support : 9
  Primary VLAN: DEFAULT_VLAN

  802.1Q VLAN ID Name          Status
  -------------- ------------- -------
  1              DEFAULT_VLAN  Static
  33             VLAN-33       Static
  44             VLAN-44       Static
```

Figure 177 Port listing for an individual VLAN

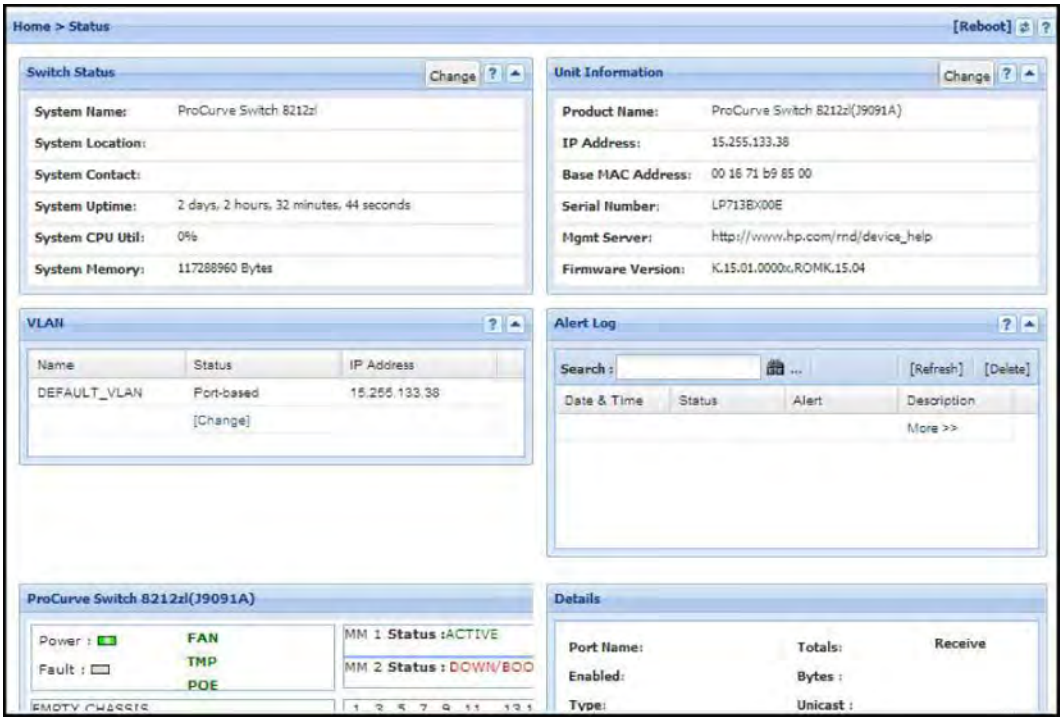


```
HP Switch(config)# show vlan 1

 Status and Counters - VLAN Information - VLAN 1

  VLAN ID : 1
  Name : DEFAULT_VLAN
  Status : Static
  Voice : Yes
  Jumbo : No

  Port Information Mode     Unknown VLAN Status
  ---------------- -------- ------------ ----------
  A1               Untagged Learn        Up
  A2               Tagged   Learn        Up
  A3               Untagged Learn        Up
  A4               Untagged Learn        Down
  A5               Untagged Learn        Up
  A6               Untagged Learn        Up
  A7               Untagged Learn        Up
```

WebAgent status information

The WebAgent Status screen provides an overview of the status of the switch. Scroll down to view more details. For information about this screen, click on **?** in the upper right corner of the WebAgent screen. For an example of a status screen, see Figure 178 (page 337).

Figure 178 Example of a WebAgent status screen



Home > Status

Switch Status

System Name: ProCurve Switch 8212zl
System Location:
System Contact:
System Uptime: 2 days, 2 hours, 32 minutes, 44 seconds
System CPU Util: 0%
System Memory: 117288960 Bytes

Unit Information

Product Name: ProCurve Switch 8212zl(J9091A)
IP Address: 15.255.133.38
Base MAC Address: 00 18 71 b9 85 00
Serial Number: LP713BX00E
Mgmt Server: http://www.hp.com/rnd/device_help
Firmware Version: K.15.01.0000x,ROMK.15.04

VLAN

Name	Status	IP Address
DEFAULT_VLAN	Port-based [Change]	15.255.133.38

Alert Log

Search :

Date & Time	Status	Alert	Description
			More >>

ProCurve Switch 8212zl(J9091A)

Power : 🟩
Fault : □
MM 1 Status :ACTIVE
MM 2 Status : DOWN/BOO

Details

Port Name:
Enabled:
Type:
Totals:
Bytes :
Unicast :

Configuring local mirroring (CLI)

Local mirroring overview

To configure a local mirroring session in which the mirroring source and destination are on the same switch, follow these general steps:

1. Determine the session and local destination port:
   - Session number (1-4) and (optional) alphanumeric name
   - Exit port (any port on the switch except a monitored interface used to mirror traffic)

CAUTION: An exit port should be connected only to a network analyzer, IDS, or other network edge device that has no connection to other network resources. Connecting a mirroring exit port to a network can result in serious network performance problems, and is strongly discouraged by HP.

2. Enter the `mirror` *`session-#`* `[name` *`session-name`* `] port` *`port-#`* command to configure the session.
3. Determine the traffic to be selected for mirroring by any of the following methods and the appropriate configuration level (VLAN, port, mesh, trunk, switch):
   - **a.** Direction: inbound, outbound, or both
   - **b.** Classifier-based mirroring policy: inbound only for IPv4 or IPv6 traffic
   - **c.** MAC source and/or destination address: inbound, outbound, or both
4. Enter the `monitor` command to assign one or more source interfaces to the session.

After you complete step 4, the switch begins mirroring traffic to the configured exit port.

Setting up local mirroring

The following commands configure mirroring for a local session in which the mirroring source and destination are on the same switch.

- The `mirror` command identifies the destination in a mirroring session.
- The `interface` and `vlan` commands identify the mirroring source, including source interface, traffic direction, and traffic-selection criteria for a specified session.

Configuring a local mirroring session

For more information, see “Configure a mirroring session on the source switch” (page 371).

Syntax:

```
[ no ] mirror 1 - 4 port exit-port-# [name name-str ]
```

The `no mirror` *`session-#`* `port` command removes the mirroring session and any mirroring source previously assigned to that session by the following commands.

Configuring traffic-direction criteria to select traffic

For more information, see “About selecting all inbound/outbound traffic to mirror” (page 373).

Syntax:

```
[ no ][ interface port/trunk/mesh  | vlan vid-#  ]monitor all
in | out | both  mirror session [ session ]... [no-tag-added]
```

Configuring ACL criteria to select inbound traffic — deprecated

Deprecated command:

Syntax:

```
[ no ][ interface port/trunk/mesh  | vlan vid-#  ]monitor ip
access-group acl-name in mirror session [ session ...]
```

Configuring a mirroring policy to select inbound traffic

For more information, see “About selecting inbound traffic using advanced classifier-based mirroring” (page 376).

Syntax:

```
class  ipv4 | ipv6 classname  [ no ][seq-number][  match |
ignore ip-protocol source-address destination-address  ]
[precedence  precedence-value][tos  tos-value][ip-dscp
codepoint][vlan  vlan-id]
```

Syntax:

```
policy mirror policy-name [no][seq-number][ class ipv4 | ipv6
classname action mirror session  ][ action mirror session
]...[ no ]
default-class action mirror session [ no ][  interface
port/trunk  | vlan vid-#  ]
service-policy mirror-policy-name in
```

In the `policy mirror` command, the `mirror` *`session`* parameter accepts a number (1 to 4) or name, if the specified mirroring session has already been configured with the name *`name-str`* option in the `mirror` command.

The `[no] interface | vlan service-policy in` command removes the mirroring policy from a port, VLAN, trunk, or mesh interface for a specified session, but leaves the session available for other assignments.

Configuring MAC-based criteria to select traffic

For more information, see “About selecting inbound/outbound traffic using a MAC address” (page 375).

Syntax:

```
[ no ] monitor mac mac-addr [  src | dst | both  ]mirror
session
```

Enter the `monitor mac mirror` command at the global configuration level.

Use the no form of the complete command syntax (for example, `no monitor mac 112233-445566 src mirror 3`) to remove a MAC address as mirroring criteria from an active session on the switch without removing the session itself.

Configuring a remote mirroring destination (CLI)

For more information, see “Configure a mirroring destination on a remote switch” (page 371).

On the remote switch

Syntax:

```
mirror endpoint ip src-ip src-udp-port dst-ip exit-port
[truncation]
```

On the local switch

For more information, see “Configure a source switch in a remote mirroring session” (page 372).

Syntax:

```
mirror session remote ip src-ip src-udp-port dst-ip
```

Configuring a local mirroring destination on the local switch (CLI)

For more information, see "Configure a source switch in a remote mirroring session" (page 372).

Syntax:

```
mirror session port exit-port
```

Configuring monitored traffic (CLI)

Deprecation of ACL-based traffic selection:

In release K.14.01 and greater, the use of ACLs to select inbound traffic in a mirroring session `interface | vlan monitor ip access-group in mirror` command has been deprecated and is replaced with classifier-based mirroring policies. For more information, see "About selecting inbound traffic using advanced classifier-based mirroring" (page 376).

Syntax:

```
interface port/trunk/mesh
```

Syntax:

```
monitor all[  in | out | both  ]mirror session [no-tag-added]
```

Syntax:

```
monitor ip access-group acl-name in mirror session ()
```

For more information, see "About selecting inbound traffic using an ACL (deprecated)" (page 374).

Syntax:

```
service-policy mirror-policy-name in
```

For more information, see "Configuring classifier-based mirroring (CLI)" (page 350).

Syntax:

```
vlan vid-#
```

Syntax:

```
monitor all[  in | out | both  ]mirror session
```

For more information, see "About selecting inbound traffic using an ACL (deprecated)" (page 374).

Syntax:

```
monitor ip access-group acl-name in mirror session ()
```

For more information, see "About selecting inbound traffic using an ACL (deprecated)" (page 374).

Syntax:

```
service-policy mirror-policy-name in
```

For more information, see "About selecting inbound traffic using an ACL (deprecated)" (page 374).

Syntax:

```
monitor mac mac-addr   src | dest | both   mirror
```

For more information, see “Configuring classifier-based mirroring (CLI)” (page 350).

Syntax:

```
show monitor [ endpoint |  session-number  | name session-name
]
```

For more information, see “Viewing a classifier-based mirroring configuration (CLI)” (page 352).

Configuring local mirroring (Menu)

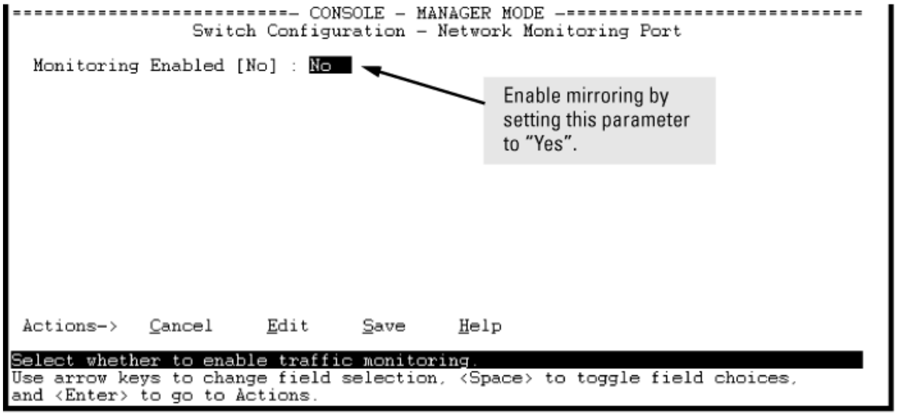
For information about local mirroring, see “Remote mirroring overview” (page 369).

NOTE: If mirroring has already been enabled on the switch, the Menu screens appear different from the one shown in this section.

Procedure 1

1. From the Main Menu, select:
   1. Switch Configuration ...
   3. Network Monitoring Port

   Figure 179 The default network mirroring configuration screen

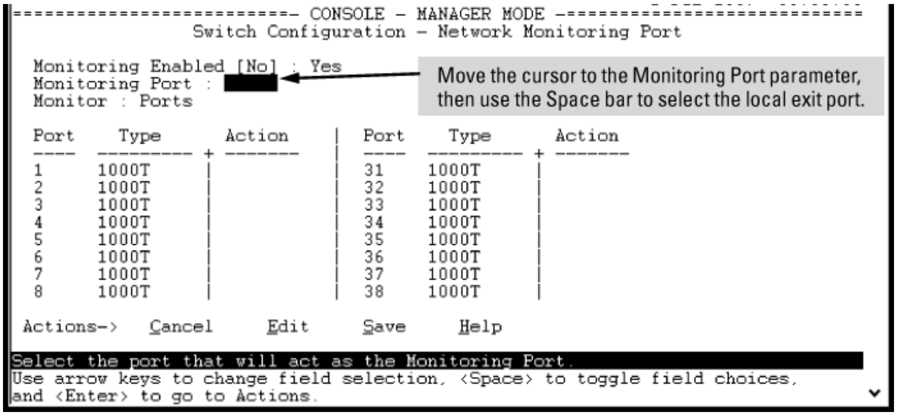


```
=========================- CONSOLE - MANAGER MODE -==========================
               Switch Configuration - Network Monitoring Port

  Monitoring Enabled [No] : No

 Actions->   Cancel     Edit     Save     Help

Select whether to enable traffic monitoring.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Enable mirroring by setting this parameter to “Yes”.

2. In the Actions menu, press **[E]** (for **Edit**).
3. If mirroring is currently disabled for session 1 (the default), enable it by pressing the Space bar (or **[Y]**) to select **Yes**.
4. Press the down arrow key to display a screen similar to Figure 180 (page 341), and move the cursor to the **Monitoring Port** parameter.

   Figure 180 How to select a local exit port



```
=========================- CONSOLE - MANAGER MODE -==========================
               Switch Configuration - Network Monitoring Port

  Monitoring Enabled [No] : Yes
  Monitoring Port :
  Monitor : Ports

  Port    Type      Action   |  Port    Type      Action
  ----  ---------- + -------- |  ----  ---------- + --------
  1     1000T      |          |  31    1000T      |
  2     1000T      |          |  32    1000T      |
  3     1000T      |          |  33    1000T      |
  4     1000T      |          |  34    1000T      |
  5     1000T      |          |  35    1000T      |
  6     1000T      |          |  36    1000T      |
  7     1000T      |          |  37    1000T      |
  8     1000T      |          |  38    1000T      |

 Actions->   Cancel     Edit     Save     Help

Select the port that will act as the Monitoring Port.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Move the cursor to the Monitoring Port parameter, then use the Space bar to select the local exit port.

5. Use the Space bar to select the port to use for sending mirrored traffic to a locally connected traffic analyzer or IDS.

   (The selected interface must be a single port. It cannot be a trunk or mesh.) In this example, port 5 is selected as the local exit port.

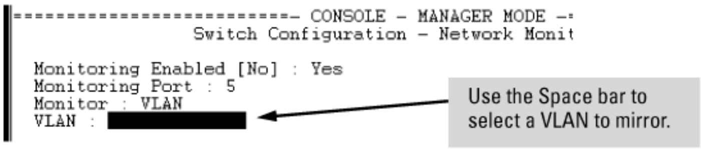
6. Highlight the Monitor field and use the Space bar to select the interfaces to mirror:

   Ports: Use for mirroring ports, static trunks, or the mesh.

   VLAN: Use for mirroring a VLAN.

7. Do one of the following:
   - If you are mirroring ports, static trunks, or the mesh, go to step 8 (page 342).
   - If you are mirroring a VLAN:

     i. Press **[Tab]** or the down arrow key to move to the **VLAN** field.



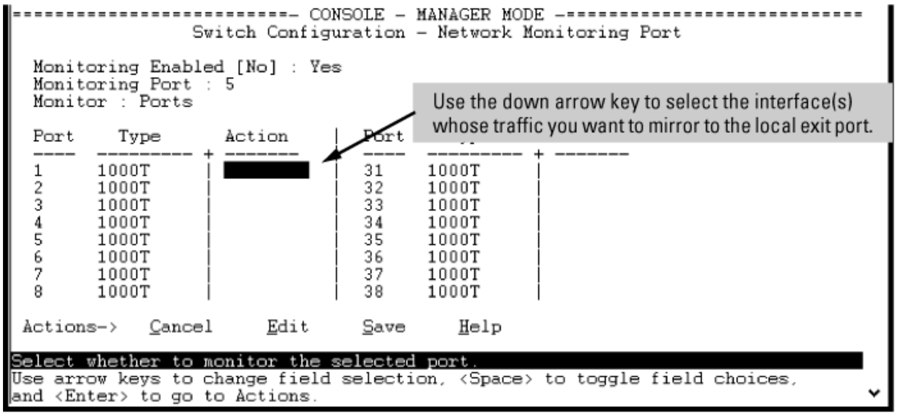
```
=========================- CONSOLE - MANAGER MODE -=
                   Switch Configuration - Network Monit

  Monitoring Enabled [No] : Yes
  Monitoring Port : 5
  Monitor : VLAN
  VLAN :
```

Use the Space bar to select a VLAN to mirror.

     ii. Use the Space bar to select the **VLAN** you want to mirror.

     iii. Go to step 10 (page 342).

8. Use the down arrow key to move the cursor to the **Action** column for the individual port interfaces and position the cursor at a port, trunk, or mesh you want to mirror.



```
=========================- CONSOLE - MANAGER MODE -===========================
                   Switch Configuration - Network Monitoring Port

  Monitoring Enabled [No] : Yes
  Monitoring Port : 5
  Monitor : Ports

  Port    Type       Action    |  Port   Type       Action
  ----  ---------- + --------  |  ----  ---------- + --------
  1     1000T      |           |  31    1000T      |
  2     1000T      |           |  32    1000T      |
  3     1000T      |           |  33    1000T      |
  4     1000T      |           |  34    1000T      |
  5     1000T      |           |  35    1000T      |
  6     1000T      |           |  36    1000T      |
  7     1000T      |           |  37    1000T      |
  8     1000T      |           |  38    1000T      |

 Actions->    Cancel     Edit     Save     Help

Select whether to monitor the selected port.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Use the down arrow key to select the interface(s) whose traffic you want to mirror to the local exit port.

9. Press the Space bar to select **Monitor** for the ports, trunks, mesh, or any combination of these that you want mirrored.

   Use the down arrow key to move from one interface to the next in the **Action** column. (If the mesh or any trunks are configured, they appear at the end of the port listing.)

10. When you finish selecting interfaces to mirror, press **[Enter]**, then press **[S]** (for **Save**) to save your changes and exit from the screen.

11. Return to the Main Menu.

Using the CLI, you can configure a mirroring session for a destination device connected to an exit port on either:

- The same switch as the source interface (local mirroring).
- A different switch (remote mirroring). The remote switch must be an HP switch offering the full mirroring capabilities described in this chapter.

△ **CAUTION:**
After you configure a mirroring session with traffic-selection criteria and a destination, the switch immediately starts to mirror traffic to each destination device connected to an exit port. In a remote mirroring session that uses IPv4 encapsulation, if the exit switch is not already configured as the destination for the session, its performance may be adversely affected by the stream of mirrored traffic. For this reason, HP Switch strongly recommends that you configure the exit switch for a remote mirroring session before configuring the source switch for the same session.

Configuring the mirroring destination on a remote switch (CLI)

For more information, see "Configure a mirroring destination on a remote switch" (page 371).

Syntax:

```
mirror endpoint ip src-ip-addr src-udp-port dst-ip-addr port
exit-port
```

Enter this command on a remote switch to configure the exit port to use in a remote mirroring session. You will configure the mirroring source on the local switch in the next step (see "Configuring the mirroring source on the local switch (CLI)" (page 343)).

The `mirror endpoint ip` command configures:

- The unique UDP port number to be used for the mirroring session on the source switch. The recommended port range is from 7933 to 65535.
- The IP address of the source switch to use in the session.
- The IP address and exit-port number on the remote (endpoint) switch.

In a remote mirroring endpoint, the IP address of exit port and the remote destination switch can belong to different VLANs.

Configuring the mirroring source on the local switch (CLI)

For more information, see "Configure a mirroring session on the source switch" (page 371).

Syntax:

```
mirror 1 - 4 [name name-str ] remote ip src-ip src-udp-port
dst-ip [truncation]
```

The `no mirror 1 - 4` command form removes both the mirroring session and any mirroring sources previously assigned to the session by the following commands.

Configuring traffic-direction criteria to select traffic (CLI)

Syntax:

```
[ no ][  interface port/trunk/mesh  | vlan vid-#  ]monitor
all  in | out | both   mirror 1 - 4 | name-str  [  1 - 4 |
name-str  ...]
```

Configuring ACL criteria to select inbound traffic

Deprecated command:

For more information, see "About selecting inbound traffic using an ACL (deprecated)" (page 374).

Syntax:

```
[ no ][ interface port/trunk/mesh  | vlan vid-#  ]monitor ip
access-group acl-name in
mirror[  1 - 4 | name-str  ][  1 - 4 | name-str  ...]
```

Configuring a mirroring policy to select inbound traffic (CLI)

For more information, see "About selecting inbound traffic using advanced classifier-based mirroring" (page 376).

Syntax:

```
class  ipv4 | ipv6 classname  [ no ][seq-number][  match |
ignore ip-protocol source-address destination-address  ]
[precedence  precedence-value][tos  tos-value][ip-dscp
codepoint][vlan  vlan-id]
```

Syntax:

```
policy mirror policy-name [no][seq-number][ class ipv4 | ipv6
classname action mirror session  ][ action mirror session
]... [ no ]
default-class action mirror session [ no ][  interface
port/trunk  | vlan vid-#  ]
service-policy mirror-policy-name in
```

In the `policy mirror` command, the `mirror` *`session`* parameter accepts a number (1 to 4) or name, if the specified mirroring session has already been configured with the name *`name-str`* option in the `mirror` command.

The
`no[  interface | vlan  ]service-policy in`
command removes the mirroring policy from a port, VLAN, trunk, or mesh interface for a specified session, but leaves the session available for other assignments.

Configuring the MAC-based criteria to select traffic (CLI)

For more information, see "About selecting inbound/outbound traffic using a MAC address" (page 375).

Syntax:

```
[ no ] monitor mac mac-addr [  src | dst | both  ]mirror
session
```

NOTE: If you have already configured session 1 with a destination, you can enter the `vlan` *`vid`* `monitor` or `interface` *`port`* `monitor` command without traffic-selection criteria and session identifier to:

- Overwrite the existing session 1 configuration.
- Automatically configure mirroring in session 1 for inbound and outbound traffic on specified VLAN or port interfaces with the preconfigured destination.

Configuring a destination switch in a remote mirroring session (CLI)

△ **CAUTION:** When configuring a remote mirroring session, *always* configure the destination switch first. Configuring the source switch first can result in a large volume of mirrored, IPv4-encapsulated traffic arriving at the destination without an exit path, which can slow switch performance.

Syntax:

```
mirror endpoint ip src-ip src-udp-port dst-ip exit-port-#
no mirror endpoint ip src-ip src-udp-port dst-ip
```

Used on a destination switch to configure the remote endpoint of a mirroring session. The command uniquely associates the mirrored traffic from the desired session on a monitored source with a remote exit port on the destination switch. You must use the same set of source and destination parameters used when you configure the same session on both the source and destination switches.

For a given mirroring session, the same *src-ip* , *src-udp-port* and *dst-ip* values must be entered with the `mirror endpoint ip` command on the destination switch, and later with the `mirror remote ip` command on the source switch. For more information, see the mirror remote ip (page 372) command syntax.

△ **CAUTION:** Do not remove the configuration of a remote mirroring endpoint support for a given session if there are source switches currently configured to mirror traffic to the endpoint.

src-ip	Must exactly match the *src-ip* address you configure on the source switch for the remote session.
src-udp-port	Must exactly match the *src-udp-port* value you configure on the source switch for the remote session. The recommended port range is 7933 to 65535. This setting associates the monitored source with the desired remote endpoint in the remote session by using the same, unique UDP port number to identify the session on the source and remote switches.
dst-ip	Must exactly match the *dst-ip* setting you configure on the source switch for the remote session.
exit-port-#	Exit port for mirrored traffic in the remote session, to which a traffic analyzer or IDS is connected.

The `no` form of the command deletes the mirroring endpoint for the configured session on the remote destination switch.

Configuring a source switch in a local mirroring session (CLI)

Enter the `mirror port` command on the source switch to configure an exit port on the same switch. To create the mirroring session, use the information gathered in "High-level overview of the mirror configuration process" (page 370).

Syntax:

```
mirror 1 - 4 port exit-port-# [name name-str ]
no mirror 1- 4
```

Assigns the exit port to use for the specified mirroring session and must be executed from the global configuration level.

`1 - 4`	Identifies the mirroring session created by this command. (Multiple sessions on the switch can use the same exit port.)	
`name` *`name-str`*	Optional alphanumeric name string used to identify the session (up to 15 characters)	
`port` *`exit-port-#`*	Exit port for mirrored traffic in the remote session. This is the port to which a traffic analyzer or IDS is connected.	

The `no` form of the command removes the mirroring session and any mirroring source previously assigned to that session. To preserve the session while deleting a mirroring source assigned to it, see the `no` command descriptions under "Configure the monitored traffic in a mirror session" (page 372).

Configuring a source switch in a remote mirroring session (CLI)

Syntax:

```
[ no ] mirror 1 - 4 [name name-str ]remote ip src-ip
src-udp-port dst-ip [truncation]
```

Used on the source switch to uniquely associate the mirrored traffic in the specified session with a remote destination switch. You must configure the same source and destination parameters when you configure the same session on both the source and destination switches. (If multiple remote sessions use the same source and destination IP addresses, each session must use a unique UDP port value.)

When you execute this command, the following message is displayed:

```
Caution: Please configure destination switch first.
         Do you want to continue [y/n]?
```

- If you have not yet configured the session on the remote destination switch, follow the configuration procedure in "Configure a mirroring destination on a remote switch" (page 371) before using this command.
- If you have already configured the session on the remote destination switch, enter **y** (for "yes") to complete this command.

`1 - 4`	Identifies the mirroring session created by this command.	
`name` *`name-str`*	Optional alphanumeric name string used as an additional session identifier (up to 15 characters).	
`src-ip`	The IP address of the VLAN or subnet on which the traffic to be mirrored enters or leaves the switch.	
`src-udp-port`	Associates the remote session with a UDP port number. When multiple sessions have the same source IP address *`src-ip`* and destination IP address *`dst-ip`* , the UDP port number must be unique in each session. The UDP port number used for a given session should be in the range of 7933 to 65535.	

	CAUTION: UDP port numbers below 7933 are reserved for various IP applications. Using them for mirroring can result in the interruption of other IP functions and in non-mirrored traffic being received on the destination switch and sent to a device connected to the remote exit port. The configured UDP port number is included in the frames mirrored from the source switch to the remote destination switch (`mirror endpoint`), and enables the remote switch to match the frames to the exit port configured for the combined UDP port number, source IP address, and destination IP address. For more information, see the `mirror endpoint ip` command syntax in "Configure a mirroring destination on a remote switch" (page 371).	
dst-ip	For the remote session specified in the command, this is the IP address of the VLAN or subnet on which the remote exit port exists. (The exit port to which a traffic analyzer or IDS is connected is configured on the remote switch in section "Configure a mirroring destination on a remote switch" (page 371).)	
`[truncation]`	Enables truncation of oversize frames, causing the part of the frame in excess of the MTU size to be truncated. Unless truncation is enabled, oversize frames are dropped. The frame size is truncated to a multiple of 18 bytes—for example, if the MTU is 1000 bytes, the frame is truncated to 990 bytes (55 * 18 bytes).	

The `no` form of the command removes the mirroring session and any mirroring source previously assigned to the session. To preserve the session while deleting a monitored source assigned to it, see the `no` command descriptions in "Configure the monitored traffic in a mirror session" (page 372).

Selecting all traffic on a port interface for mirroring according to traffic direction (CLI)

Syntax:

```
[ no ] interface port/trunk/mesh monitor all[  in | out |
both  ][ mirror 1 - 4 | name-str  ][   1 - 4 | name-str
1 - 4 | name-str     1 - 4 | name-str   ][no-tag-added]
```

Assigns a mirroring source to a previously configured mirroring session on a source switch by specifying the port, trunk, and/or mesh sources to use, the direction of traffic to mirror, and the session.

`interface` *`port/trunk/mesh`*	Identifies the source ports, static trunks, and/or mesh on which to mirror traffic. Use a hyphen for a range of consecutive ports or trunks (`a5-a8`, `Trk2-Trk4`).

	Use a comma to separate non-contiguous interfaces (`b11`, `b14`, `Trk4`, `Trk7`).
`monitor all[ in | out | both ]`	For the interface specified by *`port/trunk/mesh`* , selects traffic to mirror based on whether the traffic is entering or leaving the switch on the interface: • `in:` Mirrors entering traffic. • `out:` Mirrors exiting traffic. • `both:`Mirrors traffic entering and exiting. If you enter the `monitor all` command without selection criteria or a session identifier, the command applies by default to session 1
`mirror[ 1 - 4 | `*`name-str`*` ]`	Assigns the traffic specified by the interface and direction to a session by number or—if configured—by name. The session must have been previously configured, as described in "Configure a mirroring session on the source switch" (page 371). Depending on how many sessions are already configured on the switch, you can use the same command to assign the specified source to up to four sessions, for example, `interface a1 monitor all in mirror 1 2 4`. For limits on configuring mirroring sources in a session, see "Mirroring-source restrictions" (page 372). • `1 - 4` : Configures the selected port traffic to be mirrored in the specified session number. • `[ name `*`name-str`*` ]`: Optional; configures the selected port traffic to be mirrored in the specified session name. The string can be used interchangeably with the session number when using this command to assign a mirroring source to a session. To configure an alphanumeric name for a mirror session, see the command description in "Configure a source switch in a remote mirroring session" (page 372).
`[no-tag-added]`	Prevents a VLAN tag from being added to the mirrored copy of an outbound packet sent to a local or remote mirroring destination. For more information, see "Untagged mirrored packets" (page 373).

The no form of the command removes a mirroring source assigned to the session, but does not remove the session itself. This enables you to repurpose a session by removing an unwanted mirroring source and adding another in its place.

Selecting all traffic on a VLAN interface for mirroring according to traffic direction (CLI)

Syntax:

```
vlan vid-# monitor all[  in | out | both  ][ mirror 1 - 4 |
name-str  ][   1 - 4 | name-str     1 - 4 | name-str     1
- 4 | name-str   ]
```

This command assigns a monitored VLAN source to a previously configured mirroring session on a source switch by specifying the VLAN ID, the direction of traffic to mirror, and the session.

`vlan `*`vid-#`*	Identifies the VLAN on which to mirror traffic.
`monitor all[ in | out | both ]`	Uses the direction of traffic on the specified *`vid-#`* to select traffic to mirror. See the syntax description on (page 347). (If you enter the

	`monitor all` command without selection criteria or a session identifier, the command applies by default to session 1.
`mirror [ 1 - 4 | ` *`name-str`* ` ]`	Assigns the VLAN traffic defined by the VLAN ID and traffic direction to a session number or name. (The session must have been previously configured as described in "Configure a mirroring session on the source switch" (page 371).) Depending on how many sessions are already configured on the switch, you can use the same command to assign the specified VLAN source to up to four sessions, for example, `interface a1 monitor all in mirror 1 2 4`. For limits on configuring mirroring sources in a session, see "Mirroring-source restrictions" (page 372). • `1 - 4` : Configures the selected VLAN traffic to be mirrored in the specified session number. • `[name` *`name-str`* `]`: Optional; configures the selected port traffic to be mirrored in the specified session name. The string can be used interchangeably with the session number when using this command to assign a mirroring source to a session. To configure an alphanumeric name for a mirroring session, see the command description under "Configuring a source switch in a remote mirroring session (CLI)" (page 346).

Assigning a VLAN to a mirroring session precludes assigning any other mirroring sources to the same session. If a VLAN is already assigned to a given mirroring session, using this command to assign another VLAN to the same mirroring session results in the second assignment replacing the first. Also, if there are other (port, trunk, or mesh) mirroring sources already assigned to a session, the switch displays a message similar to:

```
Mirror source port exists on session N. Can not add mirror
source VLAN.
```

The `no` form of the command removes a mirroring source assigned to the session, but does not remove the session itself. This allows you to repurpose a session by removing an unwanted mirroring source and adding another in its place.

Configuring a MAC address to filter mirrored traffic on an interface (CLI)

For more information, see "About selecting inbound/outbound traffic using a MAC address" (page 375).

Enter the `monitor mac mirror` command at the global configuration level.

Syntax:

```
[ no ] monitor mac mac-addr [  src | dest | both  ] mirror 1
- 4 | name-str  [  1 - 4 | name-str  ][  1 - 4 | name-str  ]
[  1 - 4 | name-str  ]
```

Use this command to configure a source and/or destination MAC address as criteria for selecting traffic in one or more mirroring sessions on the switch. The MAC address you enter is configured to mirror inbound (`src`), outbound (`dest`), or both inbound and outbound (`both`) traffic on any port or learned VLAN on the switch.

`monitor mac` *`mac-addr`*	

Configures the MAC address as selection criteria for mirroring traffic on any port or learned VLAN on the switch.	
`src | dest | both`	Specifies how the MAC address is used to filter and mirror packets in inbound and/or outbound traffic on the interfaces on which the mirroring session is applied: • `src:` Mirrors all packets in inbound traffic that contain the specified MAC address as source address. • `dest:` Mirrors all packets in outbound traffic that contain the specified MAC address as destination address. **NOTE:** The MAC address of the switch is not supported as either the source or destination MAC address used to select mirrored traffic. • `both:` Mirrors all packets in both inbound and outbound traffic that contain the specified MAC address as either source or destination address.
`mirror[ 1 - 4 |` *`name-str`* `]`	Assigns the inbound and/or outbound traffic filtered by the specified MAC address to a previously configured mirroring session. The session is identified by a number or (if configured) a name. Depending on how many sessions are configured on the switch, you can use the same command to configure a MAC address as mirroring criteria in up to four sessions. To identify a session, you can enter either its name or number; for example: `mirror 1 2 3 traffsrc4` For the restrictions on how many mirroring source criteria you can configure in the same session, see "Mirroring-source restrictions" (page 372). `1 - 4 :` Specifies a mirroring session by number, for which the configured MAC address is used to select and mirror inbound and/or outbound traffic.

Packets that are sent or received on an interface configured with a mirroring session and that contain the MAC address as source and/or destination address are mirrored to a previously configured destination device.

To remove a MAC address as selection criteria in a mirroring session, you must enter the complete command syntax, for example, `no monitor mac 998877-665544 dest mirror 4`.

The `no` form of the command removes the MAC address as a mirroring criteria from an active session, but does not remove the session itself. This enables you to repurpose a session by removing an unwanted mirroring criteria and adding another in its place.

Configuring classifier-based mirroring (CLI)

For more information and a list of general steps for the process beginning with this command, see "Classifier-based mirroring configuration" (page 377). For information about restrictions on classifier-based mirroring, see "Classifier-based mirroring restrictions" (page 378).

Context: Global configuration

Syntax:

```
[ no ] class [  ipv4 | ipv6 classname  ]
```

Defines the name of a traffic class and specifies whether a policy is to be applied to IPv4 or IPv6 packets, where *`classname`* is a text string (64 characters maximum).

After you enter the `class` command, you enter the class configuration context to specify match criteria. A traffic class contains a series of `match` and `ignore` commands, which specify the criteria used to classify packets.

To configure a default traffic class, use the `default-class` command as described below. A default class manages the packets that do not match the match/ignore criteria in any other classes in a policy.

Context: Class configuration

Syntax:

```
[ no ] [seq-number] [ match | ignore ip-protocol
source-address destination-address ] [ip-dscp codepoint]
[precedence precedence-value] [tos tos-value] [vlan vlan-id]
```

For detailed information about how to enter `match` and `ignore` commands to configure a traffic class, see the "Creating a Traffic Class" section in the "Classifier-Based Software Configuration" in the *Advanced Traffic Management Guide*.

Context: Global configuration

Syntax:

```
[ no ] policy mirror policy-name
```

Defines the name of a mirroring policy and enters the policy configuration context. (For more information, see "Classifier-based mirroring configuration" (page 377).)

A traffic policy consists of one or more classes and one or more mirroring actions configured for each class of traffic. The configured actions are executed on packets that match a `match` statement in a class. No policy action is performed on packets that match an `ignore` statement.

Context: Policy configuration

Syntax:

```
[ no ] [seq-number] class [ ipv4 | ipv6 classname ]
action mirror session
```

Defines the mirroring action to be applied on a pre-configured IPv4 or IPv6 traffic class when a packet matches the `match` criteria in the traffic class. You can enter multiple `class action mirror` statements in a policy.

`[`*`seq-number`*`]`	The (optional) `seq-number` parameter sequentially orders the mirroring actions that you enter in a policy configuration. Actions are executed on matching packets in numerical order. Default: Mirroring action statements are numbered in increments of 10, starting at 10.
`class [ ipv4 | ipv6` *`classname`* `]`	Defines the preconfigured traffic class on which the mirroring actions in the policy are executed and specifies whether the mirroring policy is applied to IPv4 or IPv6 traffic in the class. The classname is a text string (64 characters maximum).
`action mirror` *`session`*	Configures mirroring for the destination and session specified by the `session` parameter.

Context: Policy configuration

Syntax:

```
[ no ] default-class action mirror session [action mirror
session ]...
```

Configures a default class that allows packets that are not matched nor ignored by any of the class configurations in a mirroring policy to be mirrored to the destination configured for the specified session.

Applying a mirroring policy on a port or VLAN interface

Enter one of the following `service-policy` commands from the global configuration context. (For more information, see "Classifier-based mirroring configuration" (page 377).)

Context: Global configuration

Syntax:

```
interface port-list service-policy policy-name in
```

Configures the specified ports with a mirroring policy that is applied to inbound traffic on each interface.

Separate individual port numbers in a series with a comma, for example, `a1,b4,d3`. Enter a range of ports by using a dash, for example, `a1-a5`.

The mirroring policy name you enter must be the same as the policy name you configured with the `policy mirror` command in the syntax (page 351).

Syntax:

```
vlan vlan-id service-policy policy-name in
```

Configures a mirroring policy on the specified VLAN that is applied to inbound traffic on the VLAN interface.

Valid VLAN ID numbers range from 1 to 4094.

The mirroring policy name you enter must be the same as the policy name you configured with the `policy mirror` command in the syntax (page 339).

For more information about how to apply a mirroring policy to an interface, see the "Applying a Service Policy to an Interface" section in the "Classifier-Based Software Configuration" chapter in the *Advanced Traffic Management Guide*.

Viewing a classifier-based mirroring configuration (CLI)

To display information about a classifier-based mirroring configuration or statistics on one or more mirroring policies, enter one of the following commands:

- `show class [ ipv4 class-name | ipv6 class-name | config ]`
- `show policy [ policy-name | config ]`
- `show policy resources`
- `show statistics policy [policy-name] [ interface port-num | vlan vid in ]`

For examples of classifier-based `show` command output, see "Classifier-based mirroring configuration" (page 377).

Viewing all mirroring sessions configured on the switch (CLI)

Syntax:

```
show monitor
```

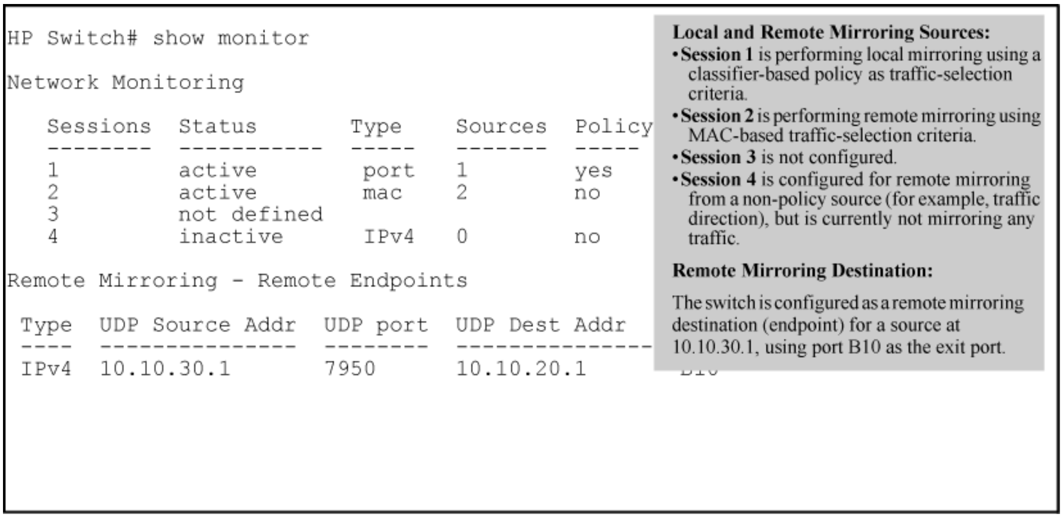
If a monitored source for a remote session is configured on the switch, the following information is displayed. Otherwise, the output displays: **Mirroring is currently disabled**.

Sessions	Lists the four configurable sessions on the switch.
Status	Displays the current status of each session : • **active:** The session is configured. • **inactive:** Only the destination has been configured; the mirroring source is not configured. • **not defined:** Mirroring is not configured for this session.
Type	Indicates whether the mirroring session is local (`port`), remote (`IPv4`), or MAC-based (`mac`) for local or remote sessions.
Sources	Indicates how many monitored source interfaces are configured for each mirroring session.
Policy	Indicates whether the source is using a classifier-based mirroring policy to select inbound IPv4 or IPv6 traffic for mirroring.

If a remote mirroring endpoint is configured on the switch, the following information is displayed. Otherwise, the output displays: **There are no Remote Mirroring endpoints currently assigned**.

Type	Indicates whether the mirroring session is local (`port`), remote (`IPv4`), or MAC-based (`mac`) for local or remote sessions.
UDP Source Addr	The IP address configured for the source VLAN or subnet on which the monitored source interface exists. In the configuration of a remote session, the same UDP source address must be configured on the source and destination switches.
UDP port	The unique UDP port number that identifies a remote session. In the configuration of a remote session, the same UDP port number must be configured on the source and destination switches.
UDP Dest Addr	The IP address configured for the destination VLAN or subnet on which the remote exit port exists. In the configuration of a remote session, the same UDP destination address must be configured on the source and destination switches.
Dest Port	Identifies the exit port for a remote session on a remote destination switch.

Figure 181 Displaying the currently configured mirroring sessions on the switch



```
HP Switch# show monitor

Network Monitoring

   Sessions  Status       Type    Sources  Policy
   --------  -----------  -----   -------  -----
   1         active        port   1        yes
   2         active        mac    2        no
   3         not defined
   4         inactive      IPv4   0        no

Remote Mirroring - Remote Endpoints

 Type  UDP Source Addr  UDP port  UDP Dest Addr
 ----  ---------------  --------  ---------------
 IPv4  10.10.30.1       7950      10.10.20.1        B10
```

Local and Remote Mirroring Sources:

- **Session 1** is performing local mirroring using a classifier-based policy as traffic-selection criteria.
- **Session 2** is performing remote mirroring using MAC-based traffic-selection criteria.
- **Session 3** is not configured.
- **Session 4** is configured for remote mirroring from a non-policy source (for example, traffic direction), but is currently not mirroring any traffic.

Remote Mirroring Destination:

The switch is configured as a remote mirroring destination (endpoint) for a source at 10.10.30.1, using port B10 as the exit port.

Viewing the remote endpoints configured on the switch (CLI)

Syntax:

`show monitor endpoint`

Displays the remote mirroring endpoints configured on the switch. Information on local sessions configured on the switch is not displayed. (To view the configuration of a local session, use the

`show monitor [  1-4 | name *name-str* ] ]`

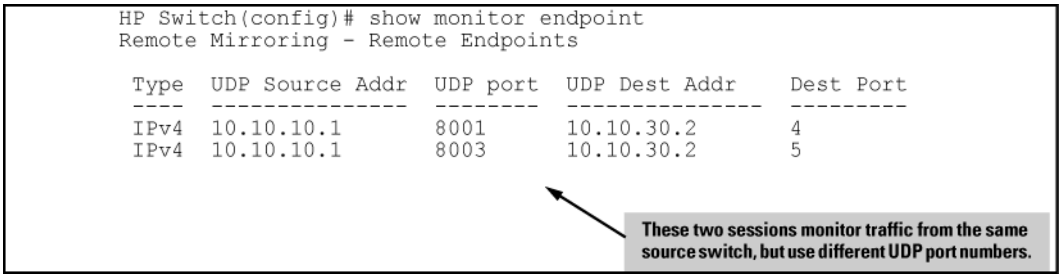
command, as described on page 74 and page 77.)

Type	Indicates whether the session is a `port` (local) or `IPv4` (remote) mirroring session.
UDP Source Addr	The IP address configured for the source VLAN or subnet on which the monitored source interface exists. In the configuration of a remote session, the same UDP source address must be configured on the source and destination switches.
UDP port	The unique UDP port number that identifies a remote session. In the configuration of a remote session, the same UDP port number must be configured on the source and destination switches.
UDP Dest Addr	The IP address configured for the destination VLAN or subnet on which the remote exit port exists. In the configuration of a remote session, the same UDP destination address must be configured on the source and destination switches.
Dest Port	fies the exit port for a remote session on a remote destination switch.

Example

In Figure 182 (page 355), the `show monitor endpoint` output shows that the switch is configured as the remote endpoint (destination) for two remote sessions from the same monitored source interface.

Figure 182 Displaying the configuration of remote mirroring endpoints on the switch



```
HP Switch(config)# show monitor endpoint
Remote Mirroring - Remote Endpoints

 Type  UDP Source Addr  UDP port  UDP Dest Addr    Dest Port
 ----  ---------------  --------  ---------------  ---------
 IPv4  10.10.10.1       8001      10.10.30.2       4
 IPv4  10.10.10.1       8003      10.10.30.2       5
```

These two sessions monitor traffic from the same source switch, but use different UDP port numbers.

Viewing the mirroring configuration for a specific session (CLI)

Syntax:

show monitor [1 - 4 | name *name-str*]

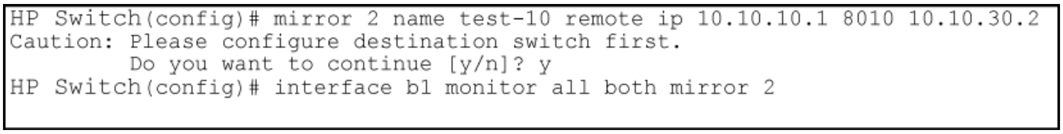
Displays detailed configuration information for a specified local or remote mirroring session on a source switch.

Session	Displays the number of the specified session.
Session Name	Displays the name of the session, if configured.
Policy	Indicates whether the source is using a classifier-based mirroring policy to select inbound IPv4 or IPv6 traffic for mirroring.
Mirroring Destination	For a local mirroring session, displays the port configured as the exit port on the source switch. For a remote mirroring session, displays IPv4, which indicates mirroring to a remote (endpoint) switch.
UDP Source Addr	The IP address configured for the source VLAN or subnet on which the monitored source interface exists. In the configuration of a remote session, the same UDP source address must be configured on the source and destination switches.
UDP port	The unique UDP port number that identifies a remote session. In the configuration of a remote session, the same UDP port number must be configured on the source and destination switches.
UDP Dest Addr	The IP address configured for the destination VLAN or subnet on which the remote exit port exists. In the configuration of a remote session, the same UDP destination address must be configured on the source and destination switches.
Status	For a remote session, displays current session activity: • **active:** The session is configured and is mirroring traffic. A remote path has been discovered to the destination. • **inactive:** The session is configured, but is not currently mirroring traffic. A remote path has *not* been discovered to the destination. • **not defined:** Mirroring is not configured for this session.
Monitoring Sources	For the specified local or remote session, displays the source (port, trunk, or VLAN) interface and the MAC address (if configured) used to select mirrored traffic.
Direction	For the selected interface, indicates whether mirrored traffic is entering the switch (in), leaving the switch (out), or both.

Viewing a remote mirroring session (CLI)

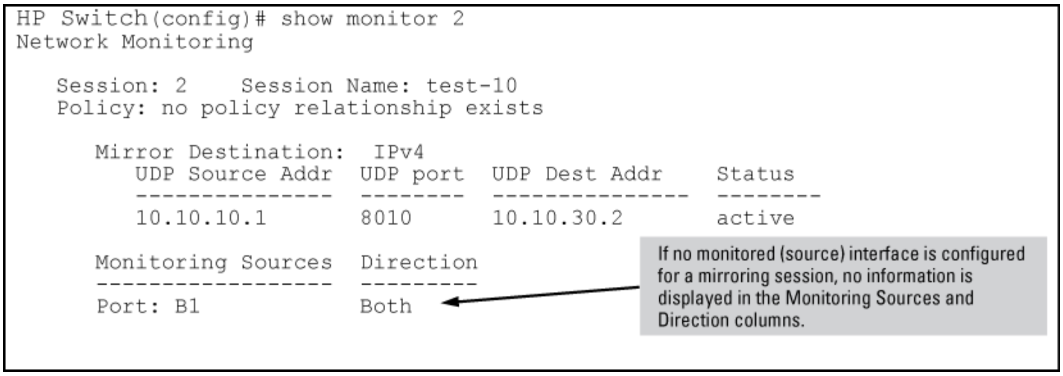
After you configure session 2 for remote mirroring (Figure 183 (page 356)), you can enter the show monitor 2 command to verify the configuration (Figure 184 (page 356)).

Figure 183 Configuring a remote mirroring session and monitored source



```
HP Switch(config)# mirror 2 name test-10 remote ip 10.10.10.1 8010 10.10.30.2
Caution: Please configure destination switch first.
         Do you want to continue [y/n]? y
HP Switch(config)# interface b1 monitor all both mirror 2
```

Figure 184 Displaying the Configuration of a Remote Mirroring Session



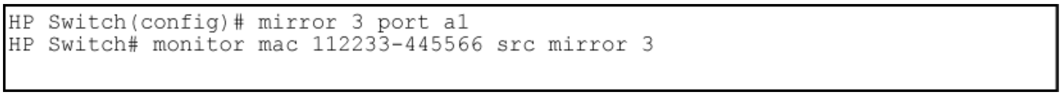
```
HP Switch(config)# show monitor 2
Network Monitoring

   Session: 2    Session Name: test-10
   Policy: no policy relationship exists

      Mirror Destination:  IPv4
         UDP Source Addr  UDP port  UDP Dest Addr    Status
         ---------------  --------  ---------------  --------
         10.10.10.1       8010      10.10.30.2       active

      Monitoring Sources  Direction
      ------------------  ---------
      Port: B1            Both
```

If no monitored (source) interface is configured for a mirroring session, no information is displayed in the Monitoring Sources and Direction columns.

Viewing a MAC-based mirroring session (CLI)

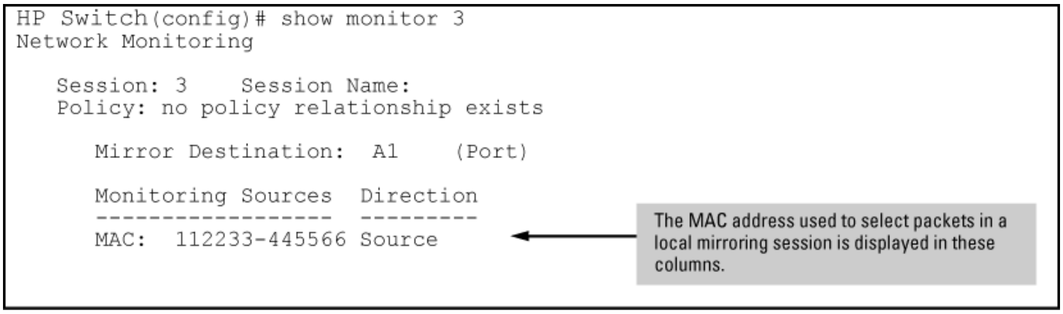
After you configure a MAC-based mirroring session (Figure 185 (page 356)), you can enter the `show monitor 3` command to verify the configuration (Figure 186 (page 356)).

Figure 185 Configuring a MAC-based mirroring session



```
HP Switch(config)# mirror 3 port a1
HP Switch# monitor mac 112233-445566 src mirror 3
```

Figure 186 Displaying a MAC-based mirroring session



```
HP Switch(config)# show monitor 3
Network Monitoring

   Session: 3    Session Name:
   Policy: no policy relationship exists

      Mirror Destination:  A1    (Port)

      Monitoring Sources  Direction
      ------------------  ---------
      MAC:  112233-445566 Source
```

The MAC address used to select packets in a local mirroring session is displayed in these columns.

Viewing a local mirroring session (CLI)

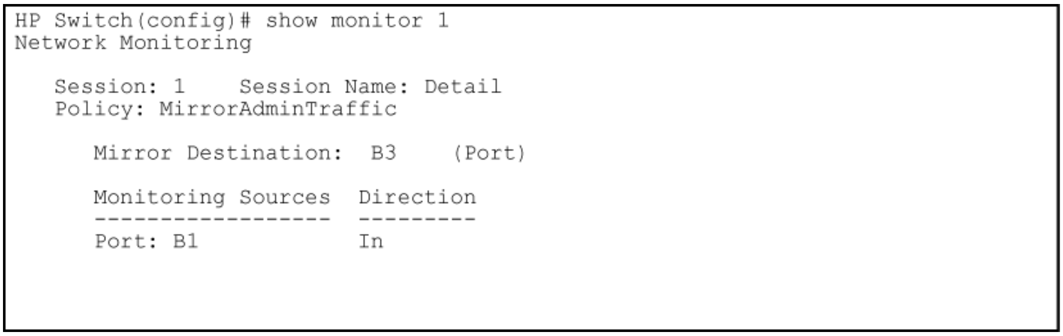
When used to display the configuration of a local session, the `show monitor` command displays a subset of the information displayed for a remote mirroring session.

Example

Figure 187 (page 357) displays a local mirroring configuration for a session configured as follows:

- Session number: 1
- Session name: Detail
- Classifier-based mirroring policy, "MirrorAdminTraffic", is used to select inbound traffic on port B1.
- Mirrored traffic is sent to exit port B3.

Figure 187 Displaying the configuration of a local mirroring session

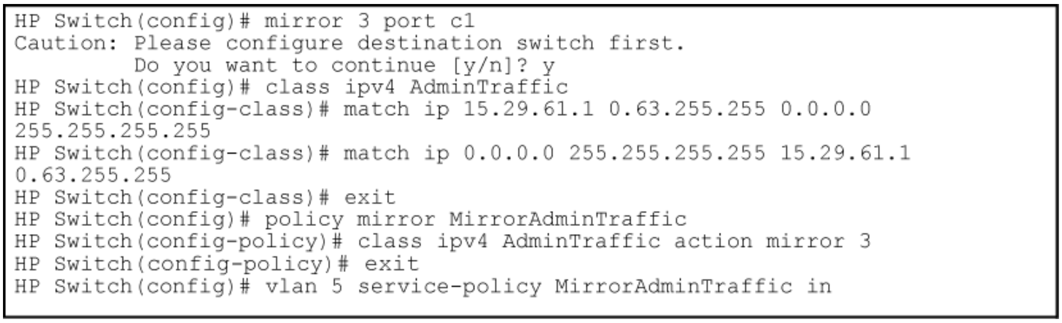


```
HP Switch(config)# show monitor 1
Network Monitoring

   Session: 1    Session Name: Detail
   Policy: MirrorAdminTraffic

      Mirror Destination:  B3    (Port)

      Monitoring Sources  Direction
      ------------------  ---------
      Port: B1            In
```

Viewing information on a classifier-based mirroring session (CLI)

In the following example, a classifier-based mirroring policy (`mirrorAdminTraffic`) mirrors selected inbound IPv4 packets on VLAN 5 to the destination device configured for mirroring session 3.

Figure 188 Configuring a classifier-based mirroring policy in a local mirroring session



```
HP Switch(config)# mirror 3 port c1
Caution: Please configure destination switch first.
         Do you want to continue [y/n]? y
HP Switch(config)# class ipv4 AdminTraffic
HP Switch(config-class)# match ip 15.29.61.1 0.63.255.255 0.0.0.0
255.255.255.255
HP Switch(config-class)# match ip 0.0.0.0 255.255.255.255 15.29.61.1
0.63.255.255
HP Switch(config-class)# exit
HP Switch(config)# policy mirror MirrorAdminTraffic
HP Switch(config-policy)# class ipv4 AdminTraffic action mirror 3
HP Switch(config-policy)# exit
HP Switch(config)# vlan 5 service-policy MirrorAdminTraffic in
```

Example 63 Displaying a classifier-based policy in a local mirroring session

```
HP Switch(config)# show monitor 3

Network Monitoring

   Session: 3   Session Name:
   Policy: MirrorAdminTraffic

     Mirror Destination:  C1   (Port)

     Monitoring Sources  Direction
     ------------------  ---------
     VLAN: 5             Source
```

Viewing information about a classifier-based mirroring configuration (CLI)

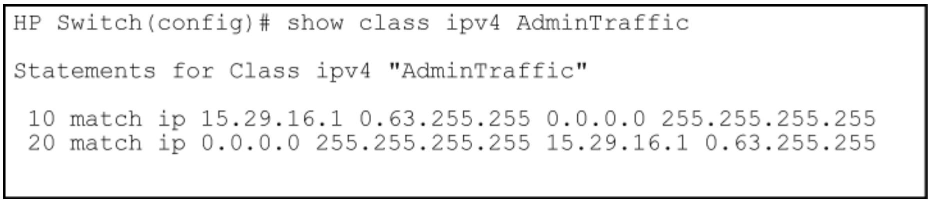
Syntax:

```
show class ipv4 classname
show class ipv6 classname
show class config
```

`ipv4` *`classname`*	Lists the statements that make up the IPv4 class identified by *`classname`*.
`ipv6` *`classname`*	Lists the statements that make up the IPv6 class identified by *`classname`*.
`config`	Displays all classes, both IPv4 and IPv6, and lists the statements that make up each class.

Additional variants of the `show class` … command provide information on classes that are members of policies that have been applied to ports or VLANs.

Figure 189 `show class` output for a mirroring policy



```
HP Switch(config)# show class ipv4 AdminTraffic

Statements for Class ipv4 "AdminTraffic"

 10 match ip 15.29.16.1 0.63.255.255 0.0.0.0 255.255.255.255
 20 match ip 0.0.0.0 255.255.255.255 15.29.16.1 0.63.255.255
```

Viewing information about a classifier-based mirroring configuration (CLI)

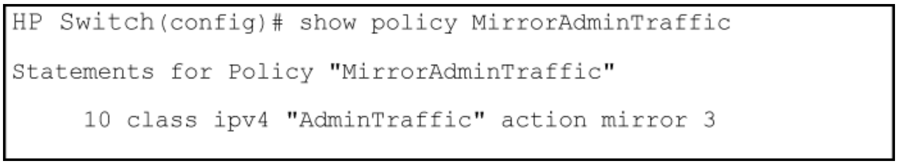
Syntax:

```
show policy policy-name
show policy config
```

`policy-name`	Lists the statements that make up the specified policy.
`config`	Displays the names of all policies defined for the switch and lists the statements that make up each policy.

Additional variants of the `show policy`… command provide information on policies that have been applied to ports or VLANs.

Figure 190 `show policy` output for a mirroring policy



```
HP Switch(config)# show policy MirrorAdminTraffic

Statements for Policy "MirrorAdminTraffic"

     10 class ipv4 "AdminTraffic" action mirror 3
```

Viewing information about statistics on one or more mirroring policies (CLI)

Syntax:

```
[  show | clear  ]statistics policy policy-name port port-num
[  show | clear  ]statistics policy policy-name vlan vid in
```

`show`	Displays the statistics for a specified policy applied to a specified port or VLAN.
`clear`	Clears statistics for the specified policy and port or VLAN.
`policy-name`	The name of the policy.
`port-num`	The number of the port on which the policy is applied (single port only, not a range).
`vid`	The number or name of the vlan on which the policy is applied. VLAN ID numbers range from 1 to 4094.
`in`	Indicates that statistics are shown for inbound traffic only.

Figure 191 (page 359) shows the number of packets (in parentheses) that have been mirrored for each match/ignore statement in the mirroring policy.

Figure 191 `show statistics policy` **output for a mirroring policy**

```
HP Switch# show statistics policy MirrorAdminTraffic vlan 30 in

HitCounts for Policy MirrorAdminTraffic

10 class ipv4 "AdminTraffic" action mirror 3

(5244)  10 match ip 15.29.16.1 0.63.255.255 0.0.0.0 255.255.255.255

(9466)  20 match ip 0.0.0.0 255.255.255.255 15.29.16.1 0.63.255.255
```

Viewing resource usage for mirroring policies (CLI)

Syntax:

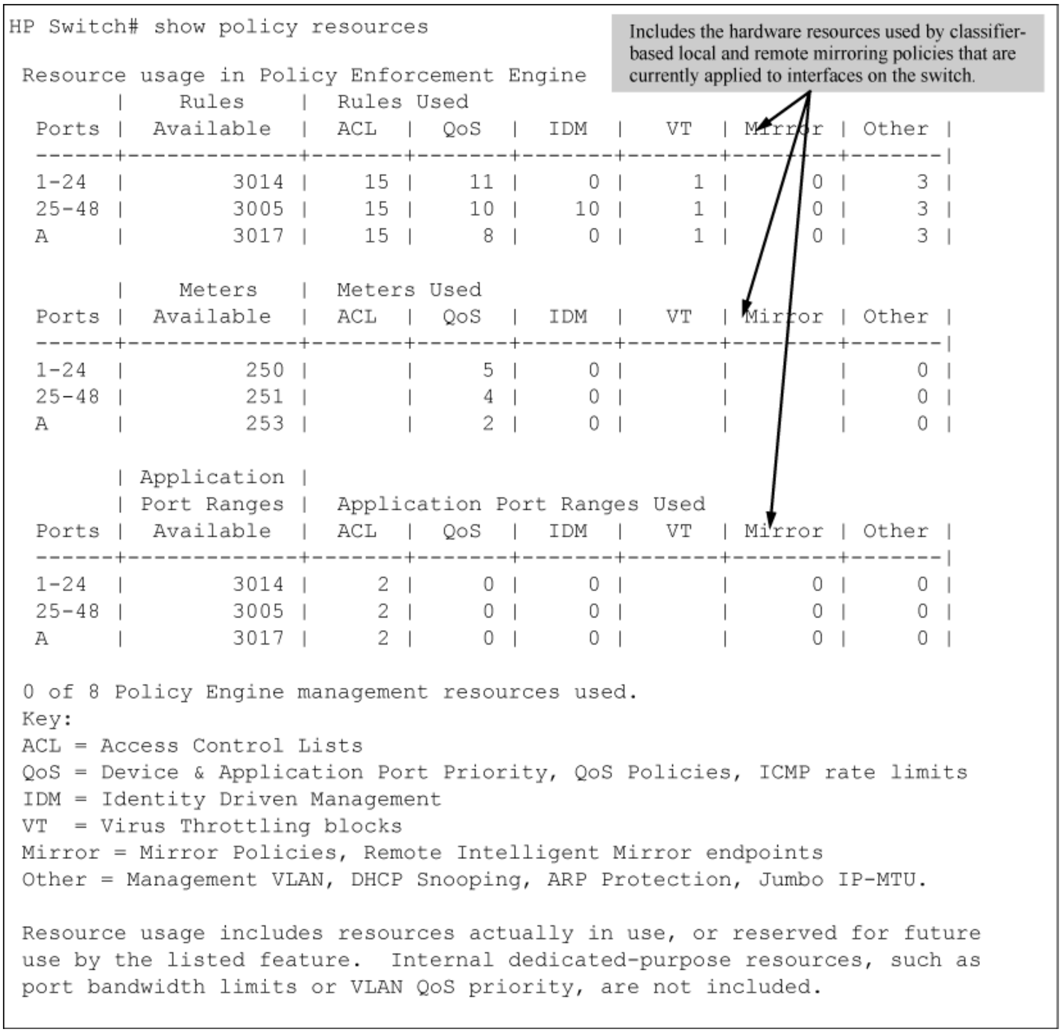
`show policy resources`

Displays the number of hardware resources (rules, meters, and application port ranges) used by classifier-based mirroring policies (local and remote) that are currently applied to interfaces on the switch, as well as QoS policies and other software features.

NOTE: The information displayed is the same as the output of the `show qos resources` and `show access-list resources` commands.

For a detailed explanation of the information displayed with the `show[ qos | access-list | policy resources ]` command, see the "Displaying current resource usage" (page 473) section in the "Monitoring Resources" (page 473) appendix.

Figure 192 Displaying the hardware resources used by currently configured mirroring policies



```
HP Switch# show policy resources

 Resource usage in Policy Enforcement Engine
       |    Rules     |  Rules Used
 Ports |  Available   |  ACL  |  QoS  |  IDM  |   VT  | Mirror | Other |
 ------+--------------+-------+-------+-------+-------+--------+-------|
 1-24  |         3014 |    15 |    11 |     0 |     1 |      0 |     3 |
 25-48 |         3005 |    15 |    10 |    10 |     1 |      0 |     3 |
 A     |         3017 |    15 |     8 |     0 |     1 |      0 |     3 |

       |    Meters    |  Meters Used
 Ports |  Available   |  ACL  |  QoS  |  IDM  |   VT  | Mirror | Other |
 ------+--------------+-------+-------+-------+-------+--------+-------|
 1-24  |          250 |       |     5 |     0 |       |        |     0 |
 25-48 |          251 |       |     4 |     0 |       |        |     0 |
 A     |          253 |       |     2 |     0 |       |        |     0 |

       | Application  |
       | Port Ranges  |  Application Port Ranges Used
 Ports |  Available   |  ACL  |  QoS  |  IDM  |   VT  | Mirror | Other |
 ------+--------------+-------+-------+-------+-------+--------+-------|
 1-24  |         3014 |     2 |     0 |     0 |       |      0 |     0 |
 25-48 |         3005 |     2 |     0 |     0 |       |      0 |     0 |
 A     |         3017 |     2 |     0 |     0 |       |      0 |     0 |

 0 of 8 Policy Engine management resources used.
 Key:
 ACL = Access Control Lists
 QoS = Device & Application Port Priority, QoS Policies, ICMP rate limits
 IDM = Identity Driven Management
 VT  = Virus Throttling blocks
 Mirror = Mirror Policies, Remote Intelligent Mirror endpoints
 Other = Management VLAN, DHCP Snooping, ARP Protection, Jumbo IP-MTU.

 Resource usage includes resources actually in use, or reserved for future
 use by the listed feature.  Internal dedicated-purpose resources, such as
 port bandwidth limits or VLAN QoS priority, are not included.
```

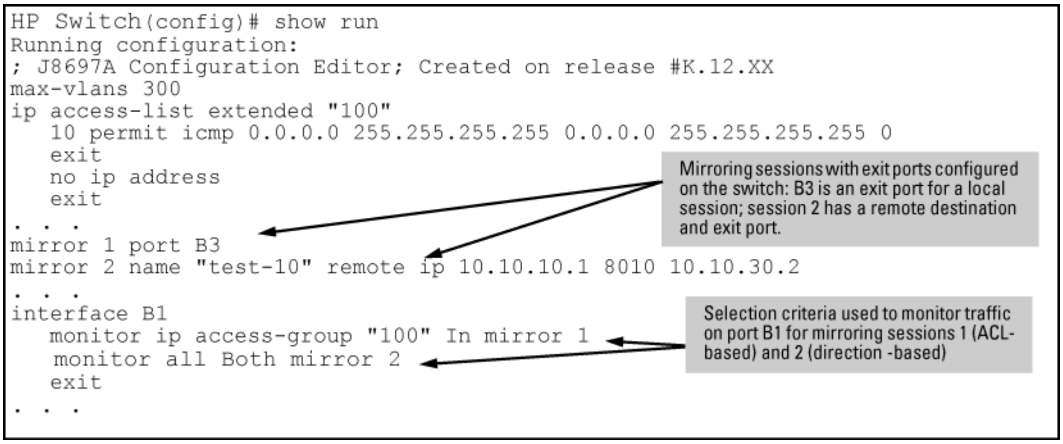
Includes the hardware resources used by classifier-based local and remote mirroring policies that are currently applied to interfaces on the switch.

Viewing the mirroring configurations in the running configuration file (CLI)

Use the `show run` command to view the current mirroring configurations on the switch. In the `show run` command output, information about mirroring sources in configured sessions begins with the `mirror` keyword; monitored source interfaces are listed per-interface.

Example

Figure 193 Displaying mirroring sources and sessions in the running configurations



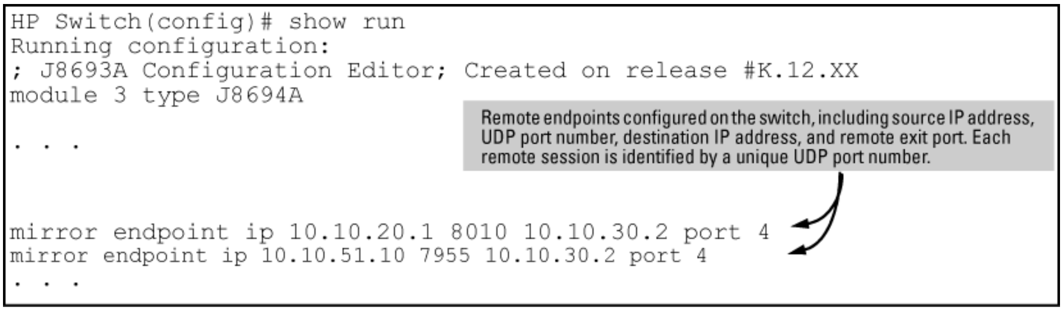
```
HP Switch(config)# show run
Running configuration:
; J8697A Configuration Editor; Created on release #K.12.XX
max-vlans 300
ip access-list extended "100"
   10 permit icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 0
   exit
   no ip address
   exit
. . .
mirror 1 port B3
mirror 2 name "test-10" remote ip 10.10.10.1 8010 10.10.30.2
. . .
interface B1
   monitor ip access-group "100" In mirror 1
   monitor all Both mirror 2
   exit
. . .
```

Mirroring sessions with exit ports configured on the switch: B3 is an exit port for a local session; session 2 has a remote destination and exit port.

Selection criteria used to monitor traffic on port B1 for mirroring sessions 1 (ACL-based) and 2 (direction -based)

Information about remote endpoints configured for remote sessions on the switch begin with the `mirror endpoint` keywords. In the following example, two remote sessions use the same exit port:

Figure 194 Displaying remote mirroring endpoints in the running configuration



```
HP Switch(config)# show run
Running configuration:
; J8693A Configuration Editor; Created on release #K.12.XX
module 3 type J8694A

. . .


mirror endpoint ip 10.10.20.1 8010 10.10.30.2 port 4
mirror endpoint ip 10.10.51.10 7955 10.10.30.2 port 4
. . .
```

Remote endpoints configured on the switch, including source IP address, UDP port number, destination IP address, and remote exit port. Each remote session is identified by a unique UDP port number.

Overview

The switches have several built-in tools for monitoring, analyzing, and troubleshooting switch and network operation:

- **Status**

  Includes options for displaying general switch information, management address data, port status, port and trunk group statistics, MAC addresses detected on each port or VLAN, and STP, IGMP, and VLAN data (page B-6 (page 323)).

- **Counters**

  Display details of traffic volume on individual ports (“Accessing port and trunk statistics (Menu)” (page 330)).

- **Event Log**

  Lists switch operating events (“Using the Event Log for troubleshooting switch problems” (page 414)).

- **Configurable trap receivers**

  Uses SNMP to enable management stations on your network to receive SNMP traps from the switch.

- **Port monitoring (mirroring)**

  Copy all traffic from the specified ports to a designated monitoring port .

NOTE: Link test and ping test—analysis tools in troubleshooting situations—are described in Appendix C, “Troubleshooting” (page 388). See “Diagnostic tools” (page 447).

Compatibility mode

Table 31 (page 361) shows how the v2 zl and zl modules behave in various combinations and situations when Compatibility mode is enabled and when it is disabled.

Table 31 Compatibility mode enabled/disabled comparisons

Modules	Compatibility mode enabled	Compatibility mode disabled
v2 zl modules only	Can insert zl module and the module will come up. Any v2 zl modules are limited to the zl configuration capacities.	v2 zl modules are at full capacity. ZL modules are not allowed to power up.
Mixed v2 zl and zl modules	Can insert zl module and the module will come up. Any v2 zl modules are limited to the zl configuration capacities.	ZL modules are not allowed to power up.

Table 31 Compatibility mode enabled/disabled comparisons *(continued)*

Modules	Compatibility mode enabled	Compatibility mode disabled
	If compatibility mode is disabled, the zl modules go down.	
ZL modules only	Same as exists already. If a v2 zl module is inserted, it operates in the same mode as the zl module, but with performance increases.	The Management Module is the only module that powers up.
	In Compatibility Mode, no v2 zl features are allowed, whether the modules are all v2 zl or not.	If Compatibility Mode is disabled and then enabled, the startup config is erased and the chassis reboots.

Port and trunk group statistics and flow control status

The features described in this section enable you to determine the traffic patterns for each port since the last reboot or reset of the switch. You can display:

- A general report of traffic on all LAN ports and trunk groups in the switch, along with the per-port flow control status (On or Off).
- A detailed summary of traffic on a selected port or trunk group.

You can also reset the counters for a specific port.

The menu interface provides a dynamic display of counters summarizing the traffic on each port. The CLI lets you see a static "snapshot" of port or trunk group statistics at a particular moment.

As mentioned above, rebooting or resetting the switch resets the counters to zero. You can also reset the counters to zero for the current session. This is useful for troubleshooting. See the (page 362), below.

NOTE: The **Reset** action resets the counter display to zero for the current session, but does not affect the cumulative values in the actual hardware counters. (In compliance with the SNMP standard, the values in the hardware counters are not reset to zero unless you reboot the switch.) Exiting from the console session and starting a new session restores the counter displays to the accumulated values in the hardware counters.

About traffic mirroring

Starting in software release K.12.xx, traffic mirroring (Intelligent Mirroring) allows you to mirror (send a copy of) network traffic received or transmitted on a switch interface to a local or remote destination, such as a traffic analyzer or IDS.

Traffic mirroring provides the following benefits:

- Allows you to monitor the traffic flow on specific source interfaces.
- Helps in analyzing and debugging problems in network operation resulting from a misbehaving network or an individual client. The mirroring of selected traffic to an external device makes it easier to diagnose a network problem from a centralized location in a topology spread across a campus.
- Supports remote mirroring to simultaneously mirror switch traffic on one or more interfaces to multiple remote destinations. (In remote mirroring, you must first configure the remote mirroring endpoint—remote switch and exit port—before you specify a mirroring source for a session.)

Mirroring terminology

Figure 195 (page 363) shows an example of the terms used to describe the configuration of a sample local and remote mirroring session:

- In the local session, inbound traffic entering Switch A is monitored on port A2 and mirrored to a destination (host), traffic analyzer 1, through exit port A15 on the switch.

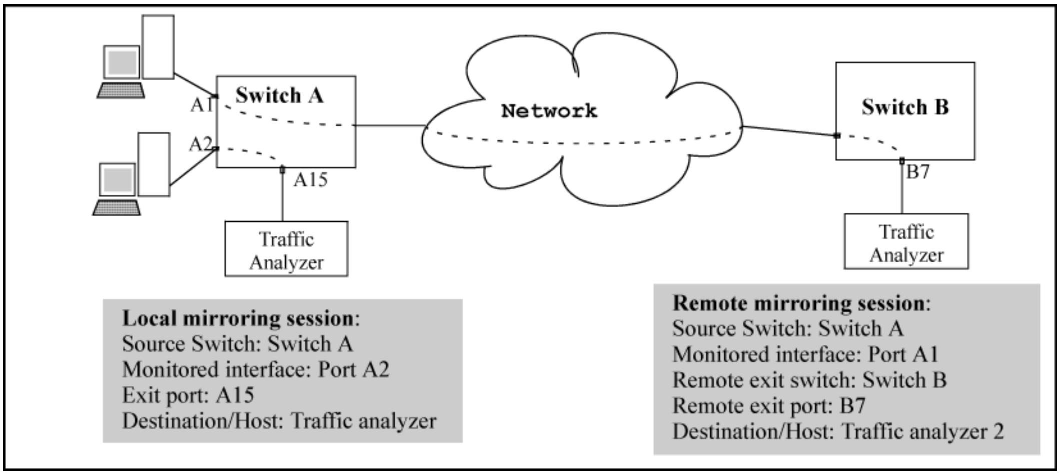
  A local mirroring session means that the monitored interface (A2) and exit port (A15) are on the same switch.

- In the remote session, inbound traffic entering Switch A is monitored on port A1. A mirrored copy of monitored traffic is routed through the network to a remote mirroring endpoint: exit port B7 on Switch B. A destination device, traffic analyzer 2, is connected to the remote exit port.

  A remote mirroring session means that:

  - The monitored interface (A1) and exit port (B7) are on different switches.
  - Mirrored traffic can be bridged or routed from a source switch to a remote switch.

Figure 195 Local and remote sessions showing mirroring terms



Local mirroring session:
Source Switch: Switch A
Monitored interface: Port A2
Exit port: A15
Destination/Host: Traffic analyzer

Remote mirroring session:
Source Switch: Switch A
Monitored interface: Port A1
Remote exit switch: Switch B
Remote exit port: B7
Destination/Host: Traffic analyzer 2

Mirroring destinations

Traffic mirroring supports destination devices that are connected to the local switch or to a remote switch:

- Traffic can be copied to a destination (host) device connected to the same switch as the mirroring source in a *local* mirroring session. You can configure up to *four* exit ports to which destination devices are connected.
- Traffic can be bridged or routed to a destination device connected to a different switch in a *remote* mirroring session. You can configure up to 32 remote mirroring endpoints (IP address and exit port) to which destination devices are connected.

Mirroring sources and sessions

Traffic mirroring supports the configuration of port and VLAN interfaces as mirroring sources in up to *four* mirroring sessions on a switch. Each session can have one or more sources (ports and/or static trunks, a mesh, or a VLAN interface) that monitor traffic entering and/or leaving the switch.

NOTE: Using the CLI, you can make full use of the switch's local and remote mirroring capabilities. Using the Menu interface, you can configure only local mirroring for either a single VLAN or a group of ports, static trunks, or both.

In remote mirroring, a 54-byte remote mirroring tunnel header is added to the front of each mirrored frame for transport from the source switch to the destination switch. This may cause some frames that were close to the MTU size to exceed the MTU size. Mirrored frames exceeding the allowed MTU size are dropped, unless the optional `[truncation]` parameter is set in the `mirror` command. For more information, including the size limitation for jumbo and non-jumbo frames, see "Maximum supported frame size" (page 384). For information on the `[truncation]` parameter, see "Configure a source switch in a remote mirroring session" (page 372).

Mirroring sessions

A mirroring session consists of a mirroring source and destination (endpoint). Although a mirroring source can be one of several interfaces, as mentioned above, for any session, the destination must be a single (exit) port. The exit port cannot be a trunk, VLAN, or mesh interface.

You can map multiple mirroring sessions to the same exit port, which provides flexibility in distributing hosts, such as traffic analyzers or an IDS. In a remote mirroring endpoint, the IP address of the exit port and the remote destination switch can belong to different VLANs.

Mirroring sessions can have the same or a different destination. You can configure an exit port on the local (source) switch and/or on a remote switch as the destination in a mirroring session. When configuring a mirroring destination, consider the following options:

- Mirrored traffic belonging to different sessions can be directed to the same destination or to different destinations.
- You can reduce the risk of oversubscribing a single exit port by:
  - Directing traffic from different session sources to multiple exit ports.
  - Configuring an exit port with a higher bandwidth than the monitored source port.
- You can segregate traffic by type, direction, or source.

Mirroring session limits

A switch running software release K.12.*xx* or greater supports the following:

- A maximum of four mirroring (local and remote) sessions.
- A maximum of 32 remote mirroring endpoints (exit ports connected to a destination device that receive mirrored traffic originating from monitored interfaces on a different switch).

Selecting mirrored traffic

You can use any of the following options to select the traffic to be mirrored on a port, trunk, mesh, or VLAN interface in a local or remote session:

- **All traffic**

  Monitors all traffic entering or leaving the switch on one or more interfaces (inbound and outbound).

- **Direction-based traffic selection**

  Monitors traffic that is either entering or leaving the switch *(inbound or outbound)*. Monitoring traffic in only one direction improves operation by reducing the amount of traffic sent to a mirroring destination.

- **MAC-based traffic selection**

  Monitors only traffic with a matching source and/or destination MAC address in packet headers entering and/or leaving the switch on one or more interfaces (*inbound and/or outbound*).

- **Classifier-based service policy**

  Provides a finer granularity of match criteria to zoom in on a subset of a monitored port or VLAN traffic (IPv4 or IPv6) and select it for local or remote mirroring (*inbound only*).

Deprecation of ACL-based traffic selection

In software release **K.14.01 or greater**, the use of ACLs for selecting traffic in a mirroring session has been deprecated and is replaced by the use of advanced classifier-based service policies (see "About selecting inbound traffic using advanced classifier-based mirroring" (page 376)).

As with ACL criteria, classifier-based match/ignore criteria allow you to limit a mirroring session to selected inbound packets on a given port or VLAN interface (instead of mirroring all inbound traffic on the interface).

The following commands have been deprecated:

- `interface` *`port/trunk/mesh`* `monitor ip access-group` *`acl-name`* `in mirror [ 1 - 4 |` *`name-str`* `]`
- `vlan` *`vid-#`* `monitor ip access-group` *`acl-name`* `in mirror[ 1 - 4 |` *`name-str`* `]`

After you install and boot release K.14.01 or greater, ACL-based local and remote mirroring sessions configured on a port or VLAN interface are automatically converted to classifier-based mirroring policies. For more information, see "Migration to release K.14.01 or greater" (page 368).

If you are running software release **K.13.xx** or earlier, ACL permit/deny criteria are supported to select IP traffic entering a switch to mirror in a local or remote session, using specified source and/or destination criteria.

Mirrored traffic destinations

Local destinations

A local mirroring traffic destination is a port on the same switch as the source of the traffic being mirrored.

Remote destinations

A *remote* mirroring traffic destination is an HP switch configured to operate as the exit switch for mirrored traffic sessions originating on other HP switches. As of June, 2007, switches capable of this operation include the following HP switches:

- 3500yl
- 5400zl
- 6200yl
- 8200zl

CAUTION:
After you configure a mirroring session with traffic-selection criteria and a destination, the switch immediately starts to mirror traffic to each destination device connected to an exit port. In a remote mirroring session that uses IPv4 encapsulation, if the intended exit switch is not already configured as the destination for the session, its performance may be adversely affected by the stream of mirrored traffic. For this reason, HP Switch strongly recommends that you configure the exit switch for a remote mirroring session before configuring the source switch for the same session.

Monitored traffic sources

You can configure mirroring for traffic entering or leaving the switch on:

- **Ports and static trunks**

  Provides the flexibility for mirroring on individual ports, groups of ports, static port trunks, or any combination of these..

- **Meshed ports**

  Enables traffic mirroring on all ports configured for meshing on the switch.

- **Static VLANs**

  Supports traffic mirroring on static VLANs configured on the switch. This option enables easy mirroring of traffic from all ports on a VLAN. It automatically adjusts mirroring to include traffic from newly added ports and to exclude traffic from ports removed from the VLAN.

Criteria for selecting mirrored traffic

On the monitored sources listed above, you can configure the following criteria to select the traffic you want to mirror:

- Direction of traffic movement (entering or leaving the switch, or both).
- Type of IPv4 or IPv6 traffic entering the switch, as defined by a classifier-based service policy (see "About selecting inbound traffic using advanced classifier-based mirroring" (page 376)).

  In software release **K.14.01 or greater**, classifier-based service policies replace ACL-based traffic selection in mirroring sessions.

- Source and/or destination MAC addresses in packet headers.

Mirroring configuration

Table 32 (page 366) shows the different types of mirroring that you can configure using the CLI, Menu, and SNMP interfaces.

Table 32 Mirroring configuration options

Monitoring interface and configuration level	**Traffic selection criteria**	**Traffic direction**		
		CLI config	**Menu and web i/f config**[1]	**Snmp config**
VLAN	All traffic	Inbound only Outbound only Both directions	All traffic (inbound and outbound combined)	Inbound only Outbound only Both directions
	ACL (IP traffic)[2]	See "About selecting inbound traffic using advanced classifier-based mirroring" (page 376).		
	Classifier-based policy (IPv4 or IPv6 traffic)	Inbound only	Not available	Not available

Port(s)
Trunk(s)
Mesh
	All traffic	Inbound only
		Outbound only
		Both directions
			All traffic (inbound and outbound combined)	Inbound only
				Outbound only
				Both directions

	ACL (IP traffic)[3]	See "About selecting inbound traffic using advanced classifier-based mirroring" (page 376).		
	Classifier-based policy (IPv4 or IPv6 traffic)	Inbound only	Not available	Not available
Switch (global)	MAC source/destination address	Inbound only	Not available	Inbound only Outbound only

Table 32 Mirroring configuration options *(continued)*

Monitoring interface and configuration level	Traffic selection criteria	Traffic direction		
		CLI config	Menu and web i/f config[1]	Snmp config
		Outbound only Both directions		Both directions

[1] Configures only session 1, and only for local mirroring.

[2] In release K.14.01 and greater, the use of ACLs to select inbound traffic in a mirroring session (using the

```
[ interface | vlan ]monitor ip access-group in mirror
```

command) has been deprecated and is replaced with classifier-based mirroring policies.

[3] In release K.14.01 and greater, the use of ACLs to select inbound traffic in a mirroring session (using the

```
[ interface | vlan ]monitor ip access-group in mirror
```

command) has been deprecated and is replaced with classifier-based mirroring policies.

Configuration notes

Using the CLI, you can configure all mirroring options on a switch.

Using the Menu, you can configure only session 1 and only local mirroring in session 1 for traffic in both directions on specified interfaces. (If session 1 has been already configured in the CLI for local mirroring for inbound-only or outbound-only traffic, and you use the Menu to modify the session 1 configuration, session 1 is *automatically* reconfigured to monitor both inbound and outbound traffic on the assigned interfaces. If session 1 has been configured in the CLI with a classifier-based mirroring policy or as a remote mirroring session, an error message is displayed if you try to use the Menu to configure the session.)

You can use the CLI can configure sessions 1 to 4 for local or remote mirroring in any combination, and override a Menu configuration of session 1.

You can also use SNMP configure sessions 1 to 4 for local or remote mirroring in any combination and override a Menu configuration of session 1, *except* that SNMP cannot be used to configure a classifier-based mirroring policy.

Remote mirroring endpoint and intermediate devices

The remote mirroring endpoint that is used in a remote mirroring session must be an HP switch that supports the mirroring functions described in this chapter. (A remote mirroring endpoint consists of the remote switch and exit port connected to a destination device.) Because remote mirroring on an HP switch uses IPv4 to encapsulate mirrored traffic sent to a remote endpoint switch, the intermediate switches and routers in a layer 2/3 domain can be from any vendor if they support IPv4.

The following restrictions apply to remote endpoint switches and intermediate devices in a network configured for traffic mirroring:

- The exit port for a mirroring destination must be an individual port and *not* a trunk, mesh, or VLAN interface.
- A switch mirrors traffic on static trunks, but *not* on dynamic LACP trunks.
- A switch mirrors traffic at line rate. When mirroring multiple interfaces in networks with high-traffic levels, it is possible to copy more traffic to a mirroring destination than the link supports. However, some mirrored traffic may not reach the destination. If you are mirroring a high-traffic volume, you can reduce the risk of oversubscribing a single exit port by:
  - Directing traffic from different session sources to multiple exit ports.
  - Configuring an exit port with a higher bandwidth than the monitored source port.

Migration to release K.12.xx

On a switch that is running a software release earlier than K.12.xx with one or more mirroring sessions configured, when you download and boot release K.12.xx, the existing mirroring configurations are managed as follows:

- A legacy mirroring configuration on a port or VLAN interface maps to session 1.
- Traffic-selection criteria for session 1 is set to `both`; both inbound and outbound traffic (traffic entering *and* leaving the switch) on the configured interface is selected for mirroring.
- In a legacy mirroring configuration, a local exit port is applied to session 1.

Booting from software versions earlier than K.12.xx

If it is necessary to boot the switch from a legacy (pre-K.12.xx) software version after using version K.12.xx or greater to configure mirroring, remove mirroring from the configuration before booting with the earlier software.

Maximum supported frame size

The IPv4 encapsulation of mirrored traffic adds a 54-byte header to each mirrored frame. If a resulting frame exceeds the MTU allowed in the path from the mirroring source to the mirroring destination, the frame is dropped, unless the optional `[truncation]` parameter is set in the `mirror` command. For more information, see "Maximum supported frame size" (page 384). For information on the `[truncation]` parameter, see "Configure a source switch in a remote mirroring session" (page 372).

Frame truncation

Mirroring does not truncate frames unless the `[truncation]` parameter in the `mirror` command is set. If that parameter is not set, oversized mirroring frames are dropped. Also, remote mirroring does not allow downstream devices in a mirroring path to fragment mirrored frames.

Migration to release K.14.01 or greater

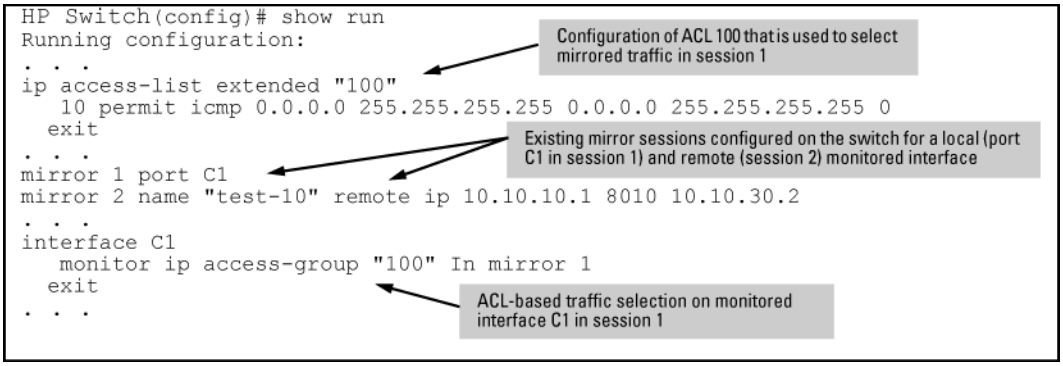
NOTE: If a switch is running software release K.12.xx, you must first upgrade to release K.13.xx before migrating the switch to release K.14.01 or greater.

When you download and boot software release K.14.01 or greater on a switch that is running release K.13.xx and has one or more mirroring sessions configured, an ACL-based mirroring configuration on a port or VLAN interface is mapped to a class and policy configuration based on the ACL.

The new mirroring policy is automatically configured on the same port or VLAN interface on which the mirroring ACL was assigned. The behavior of the new class and mirroring-policy configuration exactly matches the traffic-selection criteria and mirroring destination used in the ACL-based session .

Figure 196 (page 369) and Figure 197 (page 369) show how ACL-based selection criteria in a mirroring session are converted to a classifier-based policy and class configuration when you install release K.14.01 or greater on a switch.

Figure 196 Mirroring configuration in `show run` output in release K.13.xx



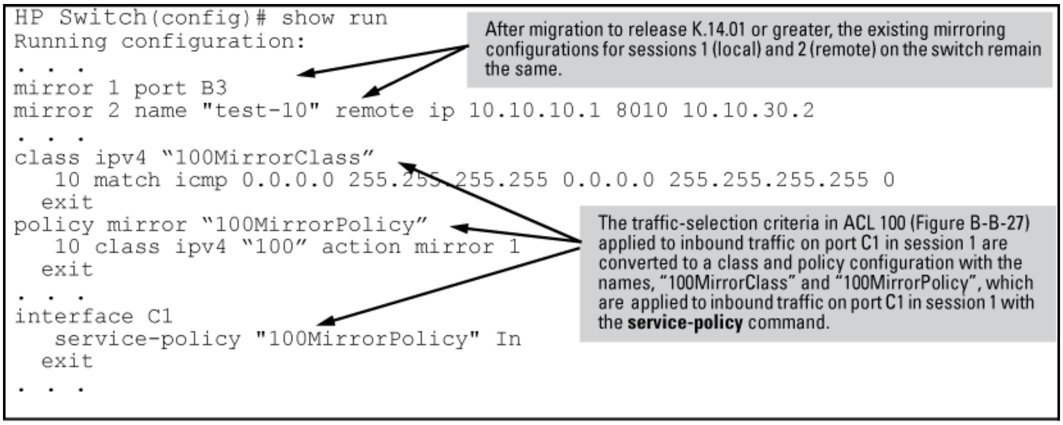
```
HP Switch(config)# show run
Running configuration:
. . .
ip access-list extended "100"
   10 permit icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 0
  exit
. . .
mirror 1 port C1
mirror 2 name "test-10" remote ip 10.10.10.1 8010 10.10.30.2
. . .
interface C1
   monitor ip access-group "100" In mirror 1
  exit
. . .
```

Configuration of ACL 100 that is used to select mirrored traffic in session 1

Existing mirror sessions configured on the switch for a local (port C1 in session 1) and remote (session 2) monitored interface

ACL-based traffic selection on monitored interface C1 in session 1

Figure 197 Mirroring configuration in `show run` output in release K.14.01 or greater



```
HP Switch(config)# show run
Running configuration:
. . .
mirror 1 port B3
mirror 2 name "test-10" remote ip 10.10.10.1 8010 10.10.30.2
. . .
class ipv4 “100MirrorClass”
   10 match icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 0
  exit
policy mirror “100MirrorPolicy”
   10 class ipv4 “100” action mirror 1
  exit
. . .
interface C1
   service-policy "100MirrorPolicy" In
  exit
. . .
```

After migration to release K.14.01 or greater, the existing mirroring configurations for sessions 1 (local) and 2 (remote) on the switch remain the same.

The traffic-selection criteria in ACL 100 (Figure B-B-27) applied to inbound traffic on port C1 in session 1 are converted to a class and policy configuration with the names, “100MirrorClass” and “100MirrorPolicy”, which are applied to inbound traffic on port C1 in session 1 with the **service-policy** command.

Using the Menu to configure local mirroring

Menu and WebAgent limits

You can use the Menu and WebAgent to quickly configure or reconfigure local mirroring on session 1 and allow one of the following two mirroring source options:

- Any combination of source ports, trunks, and a mesh.
- One static, source VLAN interface.

The Menu and WebAgent also has these limits:

- Configure and display only session 1 and only as a local mirroring session for traffic in *both* directions on the specified interface. (Selecting inbound-only or outbound-only is not an option.)
- If session 1 has been configured in the CLI for local mirroring for inbound-only or outbound-only traffic on one or more interfaces, using the Menu to change the session 1 configuration *automatically reconfigures the session* to monitor both inbound and outbound traffic on the designated interface(s).
- If session 1 has been configured in the CLI with an ACL/classifier-based mirroring policy or as a remote mirroring session, the Menu is not available for changing the session 1 configuration.
- The CLI (and SNMP) can be used to override any Menu configuration of session 1.

Remote mirroring overview

To configure a remote mirroring session in which the mirroring source and destination are on different switches, follow these general steps:

1. Determine the IP addressing, UDP port number, and destination (exit) port number for the remote session:
   - **a.** Source VLAN or subnet IP address on the source switch.
   - **b.** Destination VLAN or subnet IP address on the destination switch.
   - **c.** Random UDP port number for the session (7933-65535).
   - **d.** Remote mirroring endpoint: Exit port and IP address of the remote destination switch (In a remote mirroring endpoint, the IP address of the exit port and remote switch can belong to different VLANs. Any loopback IP address can be used except the default loopback address 127.0.0.1.)

   Requirement: For remote mirroring, the same IP addressing and UDP port number must be configured on both the source and destination switches.
2. On the remote *destination* (endpoint) switch, enter the `mirror endpoint` command with the information from step 1 (page 370) to configure a mirroring session for a specific exit port.
3. Determine the session (1 to 4) and (optional) alphanumeric name to use on the *source* switch.
4. Determine the traffic to be filtered by any of the following selection methods and the appropriate configuration level (VLAN, port, mesh, trunk, global):
   - **a.** Direction: inbound, outbound, or both.
   - **b.** Classifier-based mirroring policy: inbound only for IPv4 or IPv6 traffic.
   - **c.** MAC source and/or destination address: inbound, outbound, or both.
5. On the *source* switch:
   - **a.** Enter the `mirror` command with the session number (1 to 4) and the IP addresses and UDP port number from step 1 (page 370) to configure a mirroring session. If desired, enter the `[truncation]` parameter to allow oversize packets to be truncated rather than dropped.
   - **b.** Enter one of the following commands to configure one or more of the traffic-selection methods in step 4 (page 370) for the configured session:

     ```
     interface port/trunk/mesh [  monitor | service-policy policy-name
     in  ]
     vlan vid  [  monitor | service-policy policy-name in  ]
     monitor mac mac-addr
     ```

After you complete b, the switch begins mirroring traffic to the remote destination (endpoint) configured for the session.

Quick reference to remote mirroring setup

The commands beginning with "Configuring the mirroring destination on a remote switch (CLI)" (page 343), configure mirroring for a remote session in which the mirroring source and destination are on different switches:

- The `mirror` command identifies the destination in a mirroring session.
- The `interface` and `vlan` commands identify the monitored interface, traffic direction, and traffic-selection criteria for a specified session.

△ **CAUTION:** When configuring a remote mirroring session, always configure the destination switch first. Configuring the source switch first can result in a large volume of mirrored, IPv4-encapsulated traffic arriving at the destination without an exit path, which can slow switch performance.

High-level overview of the mirror configuration process

Determine the mirroring session and destination

For a local mirroring session

Determine the port number for the exit port (such as A5, B10, and so forth), then go to "Configure the monitored traffic in a mirror session" (page 372).

For a remote mirroring session

Determine the following information and then go to "Configure a mirroring destination on a remote switch" (page 371).

- The IP address of the VLAN or subnet on which the exit port exists on the destination switch.
- The port number of the remote exit port on the remote destination switch. (In a remote mirroring endpoint, the IP address of the exit port and the remote destination switch can belong to different VLANs.)
- The IP address of the VLAN or subnet on which the mirrored traffic enters or leaves the source switch.

△ **CAUTION:** Although the switch supports the use of UDP port numbers from 1 to 65535, UDP port numbers below 7933 are reserved for various IP applications. Using these port numbers for mirroring can result in an interruption of other IP functions, and in non-mirrored traffic being received on the destination (endpoint) switch and sent to the device connected to the remote exit port.

- The unique UDP port number to use for the session on the source switch. (The recommended port range is from 7933 to 65535.)

Configure a mirroring destination on a remote switch

This step is required only if you are configuring a remote mirroring session in which the exit port is on a different switch than the monitored (source) interface. If you are configuring local mirroring, go to "Configure a mirroring session on the source switch" (page 371).

For remote mirroring, you must configure the *destination* switch to recognize each mirroring session and forward mirrored traffic to an exit port before you configure the *source* switch. Configure the destination switch with the values you determined for remote mirroring in "High-level overview of the mirror configuration process" (page 370).

NOTE: A remote destination switch can support up to 32 remote mirroring endpoints (exit ports connected to a destination device in a remote mirroring session).

Configure a destination switch in a remote mirroring session

Enter the `mirror endpoint ip` command on the remote switch to configure the switch as a remote endpoint for a mirroring session with a different source switch. (For information on how to do this, see "Configuring a destination switch in a remote mirroring session (CLI)" (page 345).)

Configure a mirroring session on the source switch

To configure local mirroring, only a session number and exit port number are required. For more information, see "Configuring a source switch in a local mirroring session (CLI)" (page 345).

If the exit port for a mirroring destination is on a remote switch instead of the local (source) switch, you must enter the source IP address, destination IP address, and UDP port number for the remote mirroring session (see mirror remote ip (page 372)). You may also wish to enable frame truncation to allow oversize frames to be truncated rather than dropped.

Frames that exceed the maximum size (MTU) are either dropped or truncated, according to the setting of the `[truncation]` parameter in the `mirror` command. Frames that are near the MTU size may become oversize when the 54-byte remote mirroring tunnel header is added for transport between source switch and destination switch. (The addition of the header is a frequent cause for frames becoming oversize, but note that all oversize frames, whatever the cause of their excess size, are dropped or truncated.) If a frame is truncated, bytes are removed from the end of the frame. This may cause the checksum in the original frame header to fail. Some protocol analyzers may flag such a checksum mismatch as an alert.

NOTE: Note that if you enable jumbo frames to allow large frames to be transmitted, you must enable jumbo frames on all switches in the path between source and destination switches.

Configure a source switch in a remote mirroring session

Enter the `mirror remote ip` command on the source switch to configure a remote destination switch for a mirroring session on the source switch. (For information on how to do this, see "Configuring a source switch in a remote mirroring session (CLI)" (page 346). The source IP address, UDP port number, and destination IP address that you enter must be the same values that you entered with the `mirror endpoint ip` command in "Configure a mirroring destination on a remote switch" (page 371).

CAUTION: After you configure a mirroring session with traffic-selection criteria and a destination, the switch immediately starts to mirror traffic to the destination device connected to each exit port. In a remote mirroring session that uses IPv4 encapsulation, if the remote (endpoint) switch is not already configured as the destination for the session, its performance may be adversely affected by the stream of mirrored traffic. For this reason, HP Switch strongly recommends that you configure the endpoint switch in a remote mirroring session, as described in "Configure a mirroring destination on a remote switch" (page 371), before using the `mirror remote ip` command in this section to configure the mirroring source for the same session.

Configure the monitored traffic in a mirror session

This step configures one or more interfaces on a source switch with traffic-selection criteria to select the traffic to be mirrored in a local or remote session configured in section "Configure a mirroring session on the source switch" (page 371).

Traffic selection options

To configure traffic mirroring, specify the source interface, traffic direction, and criteria to be used to select the traffic to be mirrored by using the following options:

- Interface type
  - Port, trunk, and/or mesh
  - VLAN
  - Switch (global configuration level)
- Traffic direction and selection criteria
  - All inbound and/or outbound traffic on a port or VLAN interface
  - Only inbound IP traffic selected with an ACL (deprecated in software release **K.14.01 and greater**)
  - Only inbound IPv4 or IPv6 traffic selected with a classifier-based mirroring policy
  - All inbound and/or outbound traffic selected by MAC source and/or destination address

The different ways to configure traffic-selection criteria on a monitored interface are described in the following sections.

Mirroring-source restrictions

In a mirroring session, you can configure any of the following sources of mirrored traffic:

- Multiple port and trunk, and/or mesh interfaces
- One VLAN

  If you configure a VLAN as the source interface in a mirroring session and assign a second VLAN to the session, the second VLAN overwrites the first VLAN as the source of mirrored traffic.

- One classifier-based policy

  If you configure a mirroring policy on a port or VLAN interface to mirror inbound traffic in a session, you cannot configure a port, trunk, mesh, ACL, or VLAN as an additional source of mirrored traffic in the session.

- Up to 320 MAC addresses (used to select traffic according to source, destination MAC address, or both) in all mirroring sessions configured on a switch

About selecting all inbound/outbound traffic to mirror

Use the commands beginning with "Selecting all traffic on a port interface for mirroring according to traffic direction (CLI)" (page 347) and ending with "Selecting all traffic on a VLAN interface for mirroring according to traffic direction (CLI)" (page 348) to configure all inbound and/or outbound traffic on a specified VLAN, port, or trunk interfaces for a local or remote mirroring session. For an example of a mirroring configuration that selects all inbound or outbound traffic on a monitored interface, see:

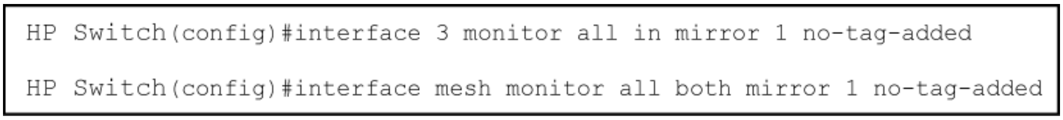
- "Example: Local mirroring using traffic-direction criteria" (page 380)
- "Example: Remote mirroring using a classifier-based policy" (page 380)

NOTE: If you have already configured session 1 with a local or remote destination (as described in "Configure a mirroring session on the source switch" (page 371)), you can enter the `vlan` *`vid`* `monitor` or `interface` *`port`* `monitor` command without additional parameters for traffic-selection criteria and session number to configure mirroring for all inbound and outbound traffic on the specified VLAN or port interfaces in session 1 with the preconfigured destination.

Untagged mirrored packets

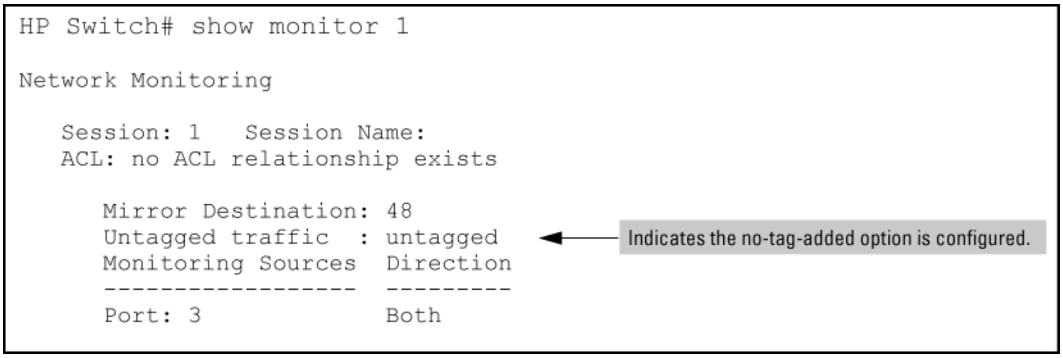
Although a VLAN tag is added (by default) to the mirrored copy of untagged outbound packets to indicate the source VLAN of the packet, it is sometimes desirable to have mirrored packets look exactly like the original packet. The `no-tag-added` parameter gives you the option of not tagging mirrored copies of outbound packets, as shown in Figure 198 (page 373) and Figure 199 (page 373).

Figure 198 Mirroring commands with the `no-tag-added` option



```
HP Switch(config)#interface 3 monitor all in mirror 1 no-tag-added

HP Switch(config)#interface mesh monitor all both mirror 1 no-tag-added
```

Figure 199 Displaying a mirror session configuration with the `no-tag-added` option



```
HP Switch# show monitor 1

Network Monitoring

   Session: 1    Session Name:
   ACL: no ACL relationship exists

      Mirror Destination: 48
      Untagged traffic  : untagged
      Monitoring Sources  Direction
      ------------------  ---------
      Port: 3             Both
```

Indicates the no-tag-added option is configured.

About using SNMP to configure `no-tag-added`

The MIB object hpicfBridgeDontTagWithVlan is used to implement the `no-tag-added` option, as shown below:

```
hpicfBridgeDontTagWithVlan OBJECT-TYPE
   SYNTAX INTEGER
```

```
      {
      enabled(1),
      disabled(2)
     }
    MAX-ACCESS  read-write
    STATUS   current
    DESCRIPTION
     "This oid mentions whether VLAN tag is part of the
    mirror'ed copy of the packet. The value ‘enabled'
    denotes that the VLAN tag shouldn't be part
    of the mirror'ed copy; ‘disabled' does put
    the VLAN tag in the mirror'ed copy. Only one
    logical port is allowed.
    This object is persistent and when written
    the entity
      SHOULD save the change to non-volatile storage."
    DEFVAL { 2 }
   ::= { hpicfBridgeMirrorSessionEntry 2 }
```

Operating notes

The following conditions apply for the `no-tag-added` option:

- The specified port can be a physical port, trunk port, or mesh port.
- Only a single logical port (physical port or trunk) can be associated with a mirror session when the `no-tag-added` option is specified. No other combination of ACL mirroring, VLAN mirroring, or port mirroring can be associated with the mirror session. If more than one logical port is specified, the following error message is displayed:

  Cannot monitor more than one logical port with no-tag-added option
- If a port changes its VLAN membership and/or untagged status within the VLAN, the "untagged port mirroring" associated with that port is updated when the configuration change is processed.
- Only four ports or trunks can be monitored at one time when all four mirror sessions are in use (one logical port per mirror session) without VLAN tags being added to a mirrored copy.
- The `no-tag-added` option can also be used when mirroring is configured with SNMP.
- A VLAN tag is still added to the copies of untagged packets obtained via VLAN-based mirroring.

About selecting inbound traffic using an ACL (deprecated)

Deprecation of ACL-based traffic selection

In release K.14.01 or greater, the use of ACLs to select inbound traffic in a mirroring session has been replaced with classifier-based mirroring policies (see “About selecting inbound traffic using advanced classifier-based mirroring” (page 376)).

The following commands have been deprecated:

- `interface` *`port/trunk/mesh`* `monitor ip access-group` *`acl-name`* `in mirror   1 - 4 |` *`name-str`*
- `vlan` *`vid-#`* `monitor ip access-group` *`acl-name`* `in mirror   1 - 4 |` *`name-str`*

After you install and boot release K.14.01 or greater, ACL-based local and remote mirroring sessions configured on a port or VLAN interface are automatically converted to classifier-based mirroring policies. For more information, see “Migration to release K.14.01 or greater” (page 368).

About selecting inbound/outbound traffic using a MAC address

Use the `monitor mac mirror` command at the global configuration level to apply a source and/or destination MAC address as the selection criteria used in a local or remote mirroring session.

While classifier-based mirroring allows you to mirror traffic using a policy to specify IP addresses as selection criteria, MAC-based mirroring allows you monitor switch traffic using a source and/or destination MAC address. You can apply MAC-based mirroring in one or more mirroring sessions on the switch to monitor:

- Inbound traffic
- Outbound traffic
- Both inbound and outbound traffic

MAC-based mirroring is useful in HP Switch Network Immunity security solutions that provide detection and response to malicious traffic at the network edge. After isolating a malicious MAC address, a security administrator can mirror all traffic sent to and received from the suspicious address for troubleshooting and traffic analysis.

The MAC address that you enter with the `monitor mac mirror` command is configured to select traffic for mirroring from all ports and learned VLANs on the switch. Therefore, a suspicions MAC address used in wireless applications can be continuously monitored as it re-appears in switch traffic on different ports or VLAN interfaces.

You can configure MAC-based mirroring from the CLI or an SNMP management station and use it to mirror:

- All inbound and outbound traffic from a group of hosts to one destination device.
- Inbound and/or outbound traffic from each host to a different destination device.
- Inbound and outbound traffic from all monitored hosts separately on two destination devices: mirroring all inbound traffic to one device and all outbound traffic to another device.

Restrictions

The following restrictions apply to MAC-based mirroring:

- Up to 320 different MAC addresses are supported for traffic selection in all mirroring sessions configured on the switch.
- A destination MAC address is not supported as mirroring criteria for routed traffic, because in routed packets, the destination MAC address is changed to the next-hop address when the packet is forwarded. Therefore, the destination MAC address that you want to mirror will not appear in routed packet headers.

  This restriction also applies to the destination MAC address of a host that is directly connected to a routing switch. (Normally, a host is connected to an edge switch, which is directly connected to the router.)

  To mirror routed traffic, we recommend that you use classifier-based policies to select IPv4 or IPv6 traffic for mirroring, as described in "About selecting inbound traffic using advanced classifier-based mirroring" (page 376).

- On a switch, you can use a MAC address only once as a source MAC address and only once as a destination MAC address to filter mirrored traffic.

  For example, after you enter the following commands:

  ```
  monitor mac 111111-222222 src mirror 1
  monitor mac 111111-222222 dest mirror 2
  ```

  The following commands are not supported:

  ```
  monitor mac 111111-222222 src mirror 3
  monitor mac 111111-222222 dest mirror 4
  ```

In addition, if you enter the `monitor mac 111111-222222 both mirror 1` command, you cannot use the MAC address `111111-222222` in any other `monitor mac mirror` configuration commands on the switch.

- To re-use a MAC address that has already been configured as a source and/or destination address for traffic selection in a mirror session, you must first remove the configuration by entering the no form of the command and then re-enter the MAC address in a new `monitor mac mirror` command.

  For example, if you have already configured MAC address `111111-222222` to filter inbound and outbound mirrored traffic, and you decide to use it to filter only inbound traffic in a mirror session, you could enter the following commands:

  ```
  monitor mac 111111-222222 both mirror 1
  no monitor mac 111111-222222 both mirror 1
  monitor mac 111111-222222 src mirror 1
  ```

- A mirroring session in which you configure MAC-based mirroring is not supported on a port, trunk, mesh, or VLAN interface on which a mirroring session with a classifier-based mirroring policy is configured.

About selecting inbound traffic using advanced classifier-based mirroring

In software release K.14.01 or greater, in addition to the traffic selection options described in "Configure the monitored traffic in a mirror session" (page 372), traffic mirroring supports the use of advanced classifier-based functions that provide:

- A finer granularity for selecting the inbound IP traffic that you want to mirror on an individual port or VLAN interface (instead of mirroring all inbound traffic on the interface)
- Support for mirroring both IPv4 and IPv6 traffic
- The ability to re-use the same traffic classes in different software-feature configurations; for example, you can apply both a QoS rate-limiting and mirroring policy on the same class of traffic.

Deprecation of ACL-based traffic selection

In software release K.14.01 or greater, advanced classifier-based policies replace ACL-based traffic selection in mirroring configurations.

Like ACL-based traffic-selection criteria, classifier-based service policies apply only to inbound traffic flows and are configured on a per-port or per-VLAN basis. In a mirroring session, classifier-based service policies do not support:

- The mirroring of outbound traffic exiting the switch
- The use of meshed ports as monitored (source) interfaces

Classifier-based mirroring is *not* designed to work with other traffic-selection methods in a mirroring session applied to a port or VLAN interface:

- If a mirroring session is already configured with one or more traffic-selection criteria (MAC-based or all inbound and/or outbound traffic), the session does not support the addition of a classifier-based policy.
- If a mirroring session is configured to use a classifier-based mirroring policy, no other traffic-selection criteria (MAC-based or all inbound and/or outbound traffic) can be added to the session on the same or a different interface.

Classifier-based mirroring policies provide greater precision when analyzing and debugging a network traffic problem. Using multiple match criteria, you can finely select and define the classes of traffic that you want to mirror on a traffic analyzer or IDS device.

For more information on how to configure and use classifier-based service policies, see the "Classifier-Based Software Configuration" chapter in the *Advanced Traffic Management Guide*.

For an example of a mirroring configuration that uses a classifier-based service policy to select traffic on a monitored interface, see "Example: Remote mirroring using a classifier-based policy" (page 380).

Classifier-based mirroring configuration

1. Evaluate the types of traffic in your network and identify the traffic types that you want to mirror.
2. Create an IPv4 or IPv6 traffic class using the `class` command to select the packets that you want to mirror in a session on a preconfigured local or remote destination device. (See "Configuring classifier-based mirroring (CLI)" (page 350).)

   A traffic class consists of match criteria, which consist of match and ignore commands.

   - `match` commands define the values that header fields must contain for a packet to belong to the class and be managed by policy actions.
   - `ignore` commands define the values which, if contained in header fields, exclude a packet from the policy actions configured for the class.

   NOTE: Be sure to enter match/ignore statements in the *precise order* in which you want their criteria to be used to check packets.

   The following match criteria are supported in match/ignore statements for inbound IPv4/IPv6 traffic:

   - IP source address (IPv4 and IPv6)
   - IP destination address (IPv4 and IPv6)
   - IP protocol (such as ICMP or SNMP)
   - Layer 3 IP precedence bits
   - Layer 3 DSCP codepoint
   - Layer 4 TCP/UDP application port (including TCP flags)
   - VLAN ID

   Enter one or more match or ignore commands from the class configuration context to filter traffic and determine the packets on which policy actions will be performed. (See (page 351).)
3. Create a mirroring policy to configure the session and destination device to which specified classes of inbound traffic are sent by entering the `policy mirror` command from the global configuration context. (See (page 339).)

   NOTE: Be sure to enter each class and its associated mirroring actions in the *precise order* in which you want packets to be checked and processed.

   To configure the mirroring actions that you want to execute on packets that match the criteria in a specified class, enter one or more class action mirror commands from the policy configuration context. (See (page 351).)

   You can configure only one mirroring session (destination) for each class. However, you can configure the same mirroring session for different classes.

   A packet that matches the match criteria in a class is mirrored to the exit (local or remote) port that has been previously configured for the session, where session is a value from **1** to **4** or a text string (if you configured the session with a name when you entered the `mirror` command).

   Prerequisite: The local or remote exit port for a session must be already configured before you enter the `mirror` *`session`* parameter in a class action statement:

   - In a local mirroring session, the exit port is configured with the `mirror` *`session-number`* `port` command.
   - In a remote mirroring session, the remote exit port is configured with the `mirror endpoint ip` and `mirror` *`session-number`* `remote ip` commands.

For more information, see “Configure a mirroring destination on a remote switch” (page 371) and “Configure a mirroring session on the source switch” (page 371).

Restriction: In a policy, you can configure only one mirroring session per class. However, you can configure the same session for different classes.

Mirroring is not executed on packets that match ignore criteria in a class.

The execution of mirroring actions is performed in the order in which the classes are numerically listed in the policy.

The complete no form of the `class action mirror` command or the `no` *`seq-number`* command removes a class and mirroring action from the policy configuration.

To manage packets that do not match the match or ignore criteria in any class in the policy, and therefore have no mirroring actions performed on them, you can enter an optional default class. The default class is placed at the end of a policy configuration and specifies the mirroring actions to perform on packets that are neither matched nor ignored.

4. (Optional) To configure a default-class in a policy, enter the `default-class` command at the end of a policy configuration and specify one or more actions to be executed on packets that are not matched and not ignored. (See “Syntax:” (page 351).)

   Prerequisite: The local or remote exit port for a session must be already configured with a destination device before you enter the `mirror` *`session`* parameter in a default-class action statement. For more information, see “Configure a mirroring destination on a remote switch” (page 371) and “Configure a mirroring session on the source switch” (page 371).

   For general information about how to configure and manage a service policy, see the "Creating a Service Policy" section in the "Classifier-Based Software Configuration" chapter in the *Advanced Traffic Management Guide*.

5. Apply the mirroring policy to inbound traffic on a port (`interface service-policy in` command) or VLAN (`vlan service-policy in` command) interface. (See

△ **CAUTION:** After you apply a mirroring policy for one or more preconfigured sessions on a port or VLAN interface, the switch immediately starts to use the traffic-selection criteria and exit port to mirror traffic to the destination device connected to each exit port.

In a remote mirroring session that uses IPv4 encapsulation, if the remote switch is not already configured as the destination for the session, its performance may be adversely affected by the stream of mirrored traffic.

For this reason, HP Switch strongly recommends that you first configure the exit switch in a remote mirroring session, as described in “Configure a mirroring destination on a remote switch” (page 371) and “Configure a mirroring session on the source switch” (page 371), before you apply a mirroring service policy on a port or VLAN interface.

Restrictions: The following restrictions apply to a mirroring service policy:

- Only one mirroring policy is supported on a port or VLAN interface.
- If you apply a mirroring policy to a port or VLAN interface on which a mirroring policy is already configured, the new policy replaces the existing one.
- A mirroring policy is supported only on inbound traffic.

Because only one mirroring policy is supported on a port or VLAN interface, ensure that the policy you want to apply contains all the required classes and actions for your configuration.

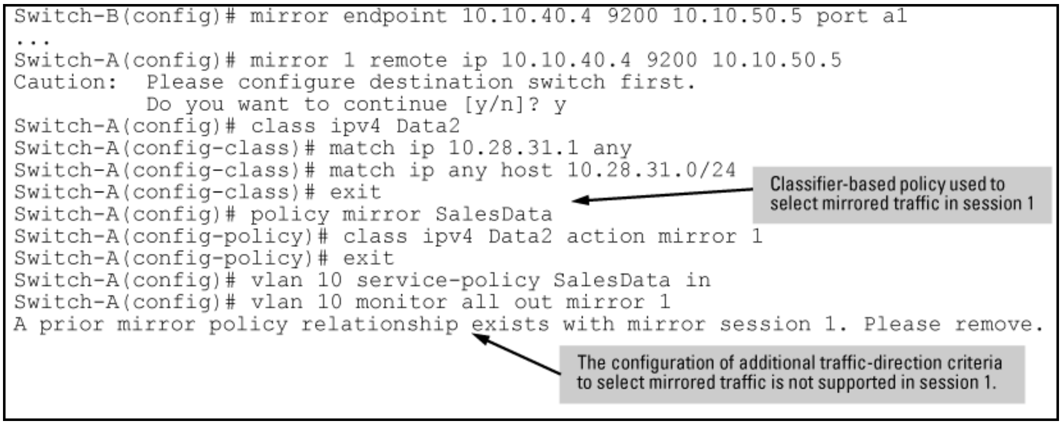
Classifier-based mirroring restrictions

The following restrictions apply to mirroring policies configured with the classifier-based model:

- A mirroring policy is supported only on *inbound* IPv4 or IPv6 traffic.
- A mirroring policy is not supported on a meshed port interface. (Classifier-based policies are supported only on a port, VLAN, or trunk interface.)
- Only one classifier-based mirroring policy is supported on a port or VLAN interface. You can, however, apply a classifier-based policy of a different type, such as QoS.

- You can enter multiple `class action mirror` statements in a policy.
  - You can configure only one mirroring session (destination) for each class.
  - You can configure the same mirroring session for different classes.
- If a mirroring session is configured with a classifier-based mirroring policy on a port or VLAN interface, no other traffic-selection criteria (MAC-based or all inbound and/or outbound traffic) can be added to the session.

Figure 200 Mirroring configuration in which only a mirroring policy is supported



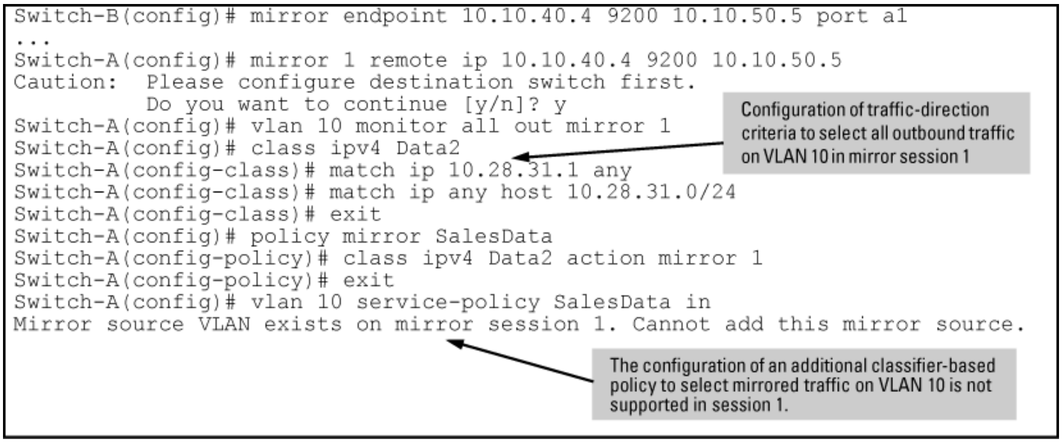
```
Switch-B(config)# mirror endpoint 10.10.40.4 9200 10.10.50.5 port a1
...
Switch-A(config)# mirror 1 remote ip 10.10.40.4 9200 10.10.50.5
Caution:  Please configure destination switch first.
          Do you want to continue [y/n]? y
Switch-A(config)# class ipv4 Data2
Switch-A(config-class)# match ip 10.28.31.1 any
Switch-A(config-class)# match ip any host 10.28.31.0/24
Switch-A(config-class)# exit
Switch-A(config)# policy mirror SalesData
Switch-A(config-policy)# class ipv4 Data2 action mirror 1
Switch-A(config-policy)# exit
Switch-A(config)# vlan 10 service-policy SalesData in
Switch-A(config)# vlan 10 monitor all out mirror 1
A prior mirror policy relationship exists with mirror session 1. Please remove.
```

Classifier-based policy used to select mirrored traffic in session 1

The configuration of additional traffic-direction criteria to select mirrored traffic is not supported in session 1.

- If a mirroring session is already configured with one or more traffic-selection criteria (MAC-based or all inbound and/or outbound traffic), the session does not support the addition of a classifier-based policy.

Figure 201 Mirroring configuration in which only traffic-selection criteria are supported



```
Switch-B(config)# mirror endpoint 10.10.40.4 9200 10.10.50.5 port a1
...
Switch-A(config)# mirror 1 remote ip 10.10.40.4 9200 10.10.50.5
Caution:  Please configure destination switch first.
          Do you want to continue [y/n]? y
Switch-A(config)# vlan 10 monitor all out mirror 1
Switch-A(config)# class ipv4 Data2
Switch-A(config-class)# match ip 10.28.31.1 any
Switch-A(config-class)# match ip any host 10.28.31.0/24
Switch-A(config-class)# exit
Switch-A(config)# policy mirror SalesData
Switch-A(config-policy)# class ipv4 Data2 action mirror 1
Switch-A(config-policy)# exit
Switch-A(config)# vlan 10 service-policy SalesData in
Mirror source VLAN exists on mirror session 1. Cannot add this mirror source.
```

Configuration of traffic-direction criteria to select all outbound traffic on VLAN 10 in mirror session 1

The configuration of an additional classifier-based policy to select mirrored traffic on VLAN 10 is not supported in session 1.

About applying multiple mirroring sessions to an interface

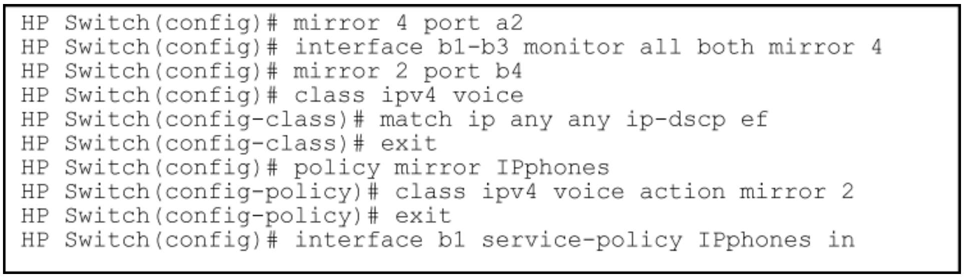
You can apply a mirroring policy to an interface that is already configured with another traffic-selection method (MAC-based or all inbound and/or outbound traffic) for a different mirroring session.

The classifier-based policy provides a finer level of granularity that allows you to zoom in on a subset of port or VLAN traffic and select it for local or remote mirroring.

In the following example, traffic on Port b1 is used as the mirroring source for two different, local mirroring sessions:

- All inbound and outbound traffic on Ports b1, b2, and b3 is mirrored in session 4.
- Only selected voice traffic on Port b1 is mirrored in session 2.

Figure 202 Example of applying multiple sessions to the same interface



```
HP Switch(config)# mirror 4 port a2
HP Switch(config)# interface b1-b3 monitor all both mirror 4
HP Switch(config)# mirror 2 port b4
HP Switch(config)# class ipv4 voice
HP Switch(config-class)# match ip any any ip-dscp ef
HP Switch(config-class)# exit
HP Switch(config)# policy mirror IPphones
HP Switch(config-policy)# class ipv4 voice action mirror 2
HP Switch(config-policy)# exit
HP Switch(config)# interface b1 service-policy IPphones in
```

Mirroring configuration examples

Example: Local mirroring using traffic-direction criteria

An administrator wants to mirror the inbound traffic from workstation "X" on port A5 and workstation "Y" on port B17 to a traffic analyzer connected to port C24 (see Figure 203 (page 380)). In this case, the administrator chooses "1" as the session number. (Any unused session number from 1 to 4 is valid.) Because the switch provides both the source and destination for the traffic to monitor, local mirroring can be used. In this case, the command sequence is:

1. Configure the local mirroring session, including the exit port.
2. Configure the monitored source interfaces for the session.

Figure 203 Local mirroring topology

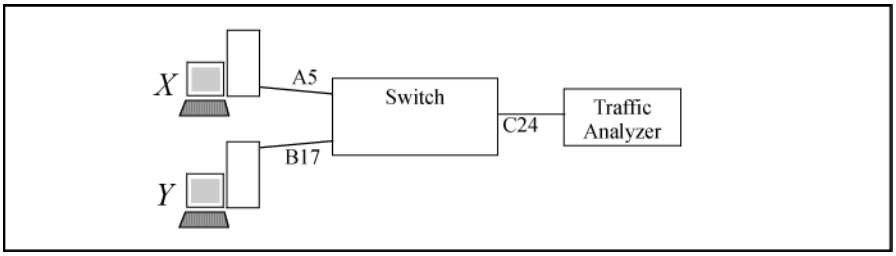
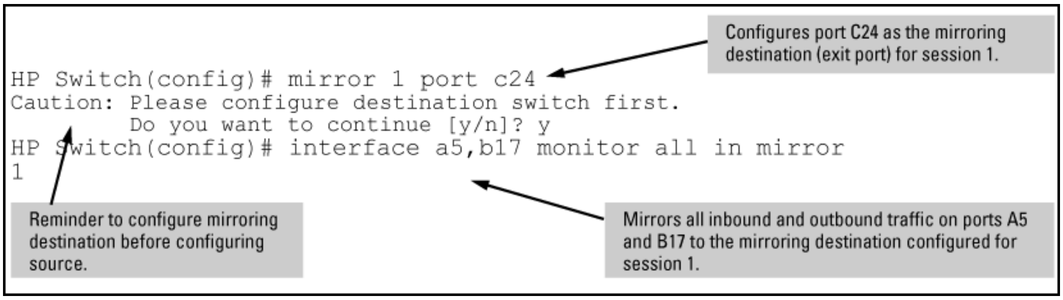


Figure 204 Configuring a local mirroring session for all inbound and outbound port traffic



```
HP Switch(config)# mirror 1 port c24
Caution: Please configure destination switch first.
         Do you want to continue [y/n]? y
HP Switch(config)# interface a5,b17 monitor all in mirror
1
```

Configures port C24 as the mirroring destination (exit port) for session 1.

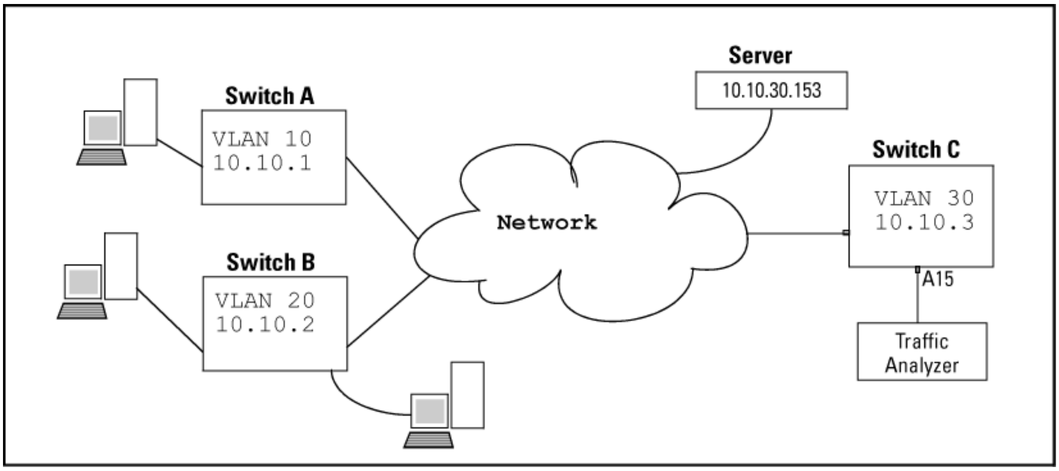
Reminder to configure mirroring destination before configuring source.

Mirrors all inbound and outbound traffic on ports A5 and B17 to the mirroring destination configured for session 1.

Example: Remote mirroring using a classifier-based policy

In the network shown in Figure 205 (page 381), an administrator has connected a traffic analyzer to port A15 (in VLAN 30) on switch C to monitor the TCP traffic to the server at 10.10.30.153 from workstations connected to switches A and B. Remote mirroring sessions are configured on switches A and B, and a remote mirroring endpoint on switch C. TCP traffic is routed through the network to the server from VLANs 10 and 20 on VLAN 30.

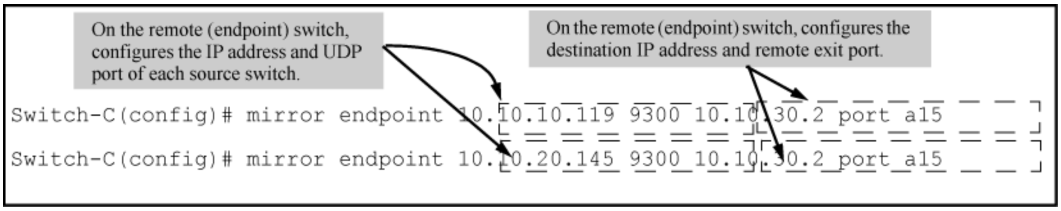
Figure 205 Sample topology in a remote mirroring session



To configure this remote mirroring session using a classifier-based policy to select inbound TCP traffic on two VLAN interfaces, take the following steps:

1. On remote switch C, configure a remote mirroring endpoint using port A15 as the exit port (as described in "Configure a mirroring destination on a remote switch" (page 371)).

   Figure 206 Configuring a remote mirroring endpoint: remote switch and exit port

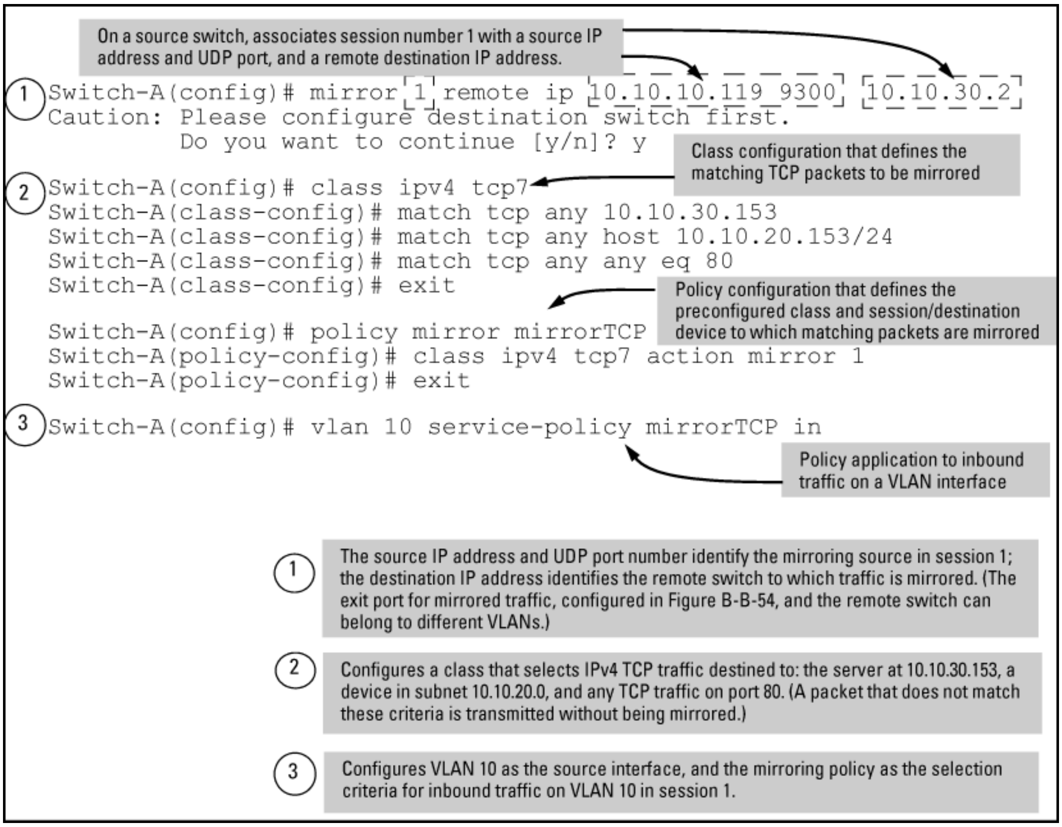
   On the remote (endpoint) switch, configures the IP address and UDP port of each source switch.

   On the remote (endpoint) switch, configures the destination IP address and remote exit port.

```
Switch-C(config)# mirror endpoint 10.10.10.119 9300 10.10.30.2 port a15
Switch-C(config)# mirror endpoint 10.10.20.145 9300 10.10.30.2 port a15
```

2. On source switch A, configure an association between the remote mirroring endpoint on switch C and a mirroring session on switch A (as described in "Configure a mirroring session on the source switch" (page 371)).
3. On switch A, configure a classifier-based mirroring policy to select inbound TCP traffic destined to the server at 10.10.30.153, and apply the policy to the interfaces of VLAN 10 (as described in "About selecting inbound traffic using advanced classifier-based mirroring" (page 376)).

Figure 207 Configuring a classifier-based policy on source switch A



On a source switch, associates session number 1 with a source IP address and UDP port, and a remote destination IP address.

```
Switch-A(config)# mirror 1 remote ip 10.10.10.119 9300 10.10.30.2
Caution: Please configure destination switch first.
         Do you want to continue [y/n]? y

Switch-A(config)# class ipv4 tcp7
Switch-A(class-config)# match tcp any 10.10.30.153
Switch-A(class-config)# match tcp any host 10.10.20.153/24
Switch-A(class-config)# match tcp any any eq 80
Switch-A(class-config)# exit

Switch-A(config)# policy mirror mirrorTCP
Switch-A(policy-config)# class ipv4 tcp7 action mirror 1
Switch-A(policy-config)# exit

Switch-A(config)# vlan 10 service-policy mirrorTCP in
```

Class configuration that defines the matching TCP packets to be mirrored

Policy configuration that defines the preconfigured class and session/destination device to which matching packets are mirrored

Policy application to inbound traffic on a VLAN interface

1 The source IP address and UDP port number identify the mirroring source in session 1; the destination IP address identifies the remote switch to which traffic is mirrored. (The exit port for mirrored traffic, configured in Figure B-B-54, and the remote switch can belong to different VLANs.)

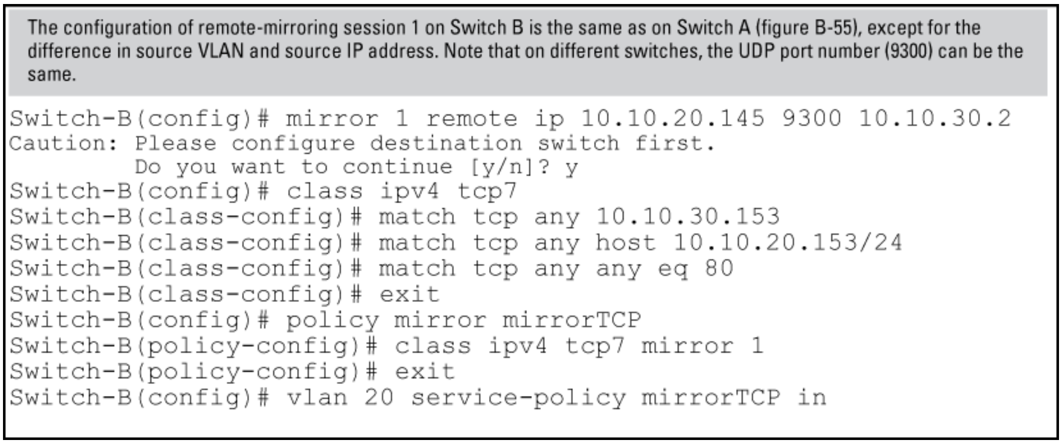
2 Configures a class that selects IPv4 TCP traffic destined to: the server at 10.10.30.153, a device in subnet 10.10.20.0, and any TCP traffic on port 80. (A packet that does not match these criteria is transmitted without being mirrored.)

3 Configures VLAN 10 as the source interface, and the mirroring policy as the selection criteria for inbound traffic on VLAN 10 in session 1.

4. On source switch B, repeat steps 2 and 3:
   a. Configure an association between the remote mirroring endpoint on switch C and a mirroring session on switch B.
   b. Configure a classifier-based mirroring policy to select inbound TCP traffic destined to the server at 10.10.30.153, and apply the policy to a VLAN interface for VLAN 20.

Because the remote session has mirroring sources on different switches, you can use the same session number (1) for both sessions.

Figure 208 Configuring a classifier-based policy on source switch B



The configuration of remote-mirroring session 1 on Switch B is the same as on Switch A (figure B-55), except for the difference in source VLAN and source IP address. Note that on different switches, the UDP port number (9300) can be the same.

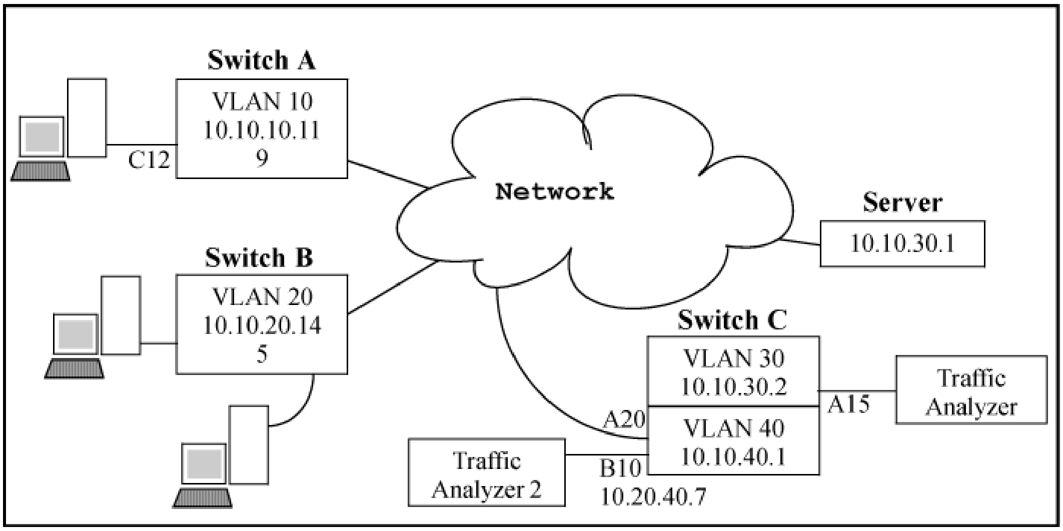
```
Switch-B(config)# mirror 1 remote ip 10.10.20.145 9300 10.10.30.2
Caution: Please configure destination switch first.
        Do you want to continue [y/n]? y
Switch-B(config)# class ipv4 tcp7
Switch-B(class-config)# match tcp any 10.10.30.153
Switch-B(class-config)# match tcp any host 10.10.20.153/24
Switch-B(class-config)# match tcp any any eq 80
Switch-B(class-config)# exit
Switch-B(config)# policy mirror mirrorTCP
Switch-B(policy-config)# class ipv4 tcp7 mirror 1
Switch-B(policy-config)# exit
Switch-B(config)# vlan 20 service-policy mirrorTCP in
```

Example: Remote mirroring using traffic-direction criteria

In the network shown in Figure 209 (page 383), the administrator connects another traffic analyzer to port B10 (in VLAN 40) on switch C to monitor all traffic entering switch A on port C12. For this mirroring configuration, the administrator configures a mirroring destination (with a remote exit port of B10) on switch C, and a remote mirroring session on switch A.

If the mirroring configuration in the proceeding example is enabled, it is necessary to use a different session number (2) and UDP port number (9400). (The IP address of the remote exit port [10.10.40.7] connected to traffic analyzer 2 [exit port B10] can belong to a different VLAN than the destination IP address of the VLAN used to reach remote switch C [10.20.40.1]).

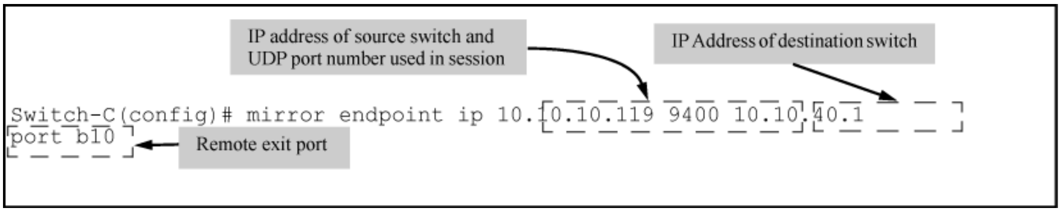
Figure 209 Sample topology for remote mirroring from a port interface



To configure this remote mirroring session using a directional-based traffic selection on a port interface, the operator must take the following steps:

1. On remote switch C, configure the remote mirroring endpoint using port B10 as the exit port for a traffic analyzer (as described in "Configure a mirroring destination on a remote switch" (page 371)):

   Figure 210 Configuring a remote mirroring endpoint



```
Switch-C(config)# mirror endpoint ip 10.10.10.119 9400 10.10.40.1
port b10
```

IP address of source switch and UDP port number used in session

IP Address of destination switch

Remote exit port

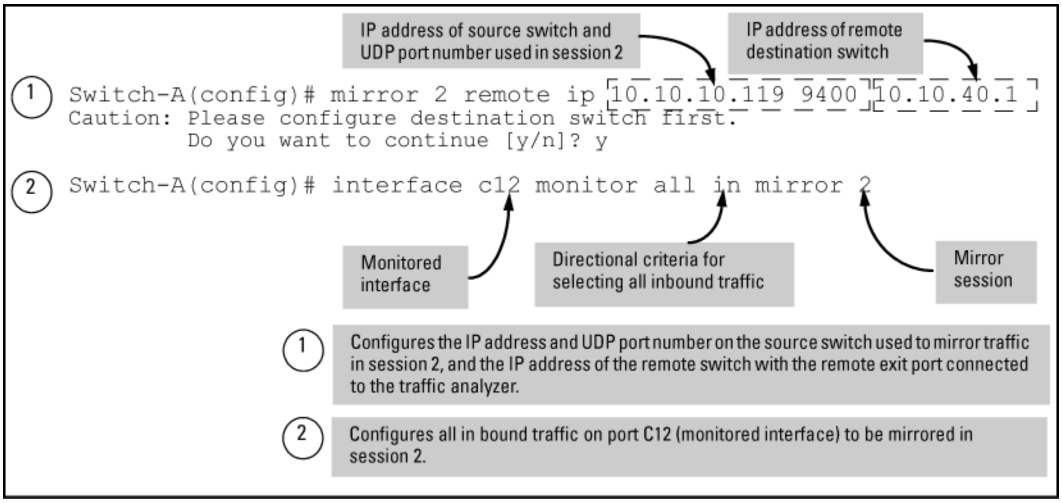
2. On source switch A, configure session 2 to use UDP port 9400 to reach the remote mirroring endpoint on switch C (10.10.40.1):

```
mirror 2 remote ip 10.10.10.119 9400 10.10.40.1
```

3. On source switch A, configure the local port C12 to select all inbound traffic to send to the preconfigured mirroring destination for session 2:

   ```
   interface c12 monitor all in mirror 2
   ```

Figure 211 Configuring a remote mirroring session for inbound port traffic



```
1  Switch-A(config)# mirror 2 remote ip 10.10.10.119 9400 10.10.40.1
   Caution: Please configure destination switch first.
            Do you want to continue [y/n]? y

2  Switch-A(config)# interface c12 monitor all in mirror 2
```

IP address of source switch and UDP port number used in session 2
IP address of remote destination switch
Monitored interface
Directional criteria for selecting all inbound traffic
Mirror session

1 Configures the IP address and UDP port number on the source switch used to mirror traffic in session 2, and the IP address of the remote switch with the remote exit port connected to the traffic analyzer.

2 Configures all in bound traffic on port C12 (monitored interface) to be mirrored in session 2.

Maximum supported frame size

The IPv4 encapsulation of mirrored traffic adds a 54-byte header to each mirrored frame. If a resulting frame exceeds the MTU allowed in the network, the frame is dropped or truncated.

NOTE: Oversized mirroring frames are dropped or truncated, according to the setting of the `[truncation]` parameter in the `mirror` command. Also, remote mirroring does not allow downstream devices in a mirroring path to fragment mirrored frames.

If jumbo frames are enabled on the mirroring source switch, the mirroring destination switch and all downstream devices connecting the source switch to the mirroring destination must be configured to support jumbo frames.

Enabling jumbo frames to increase the mirroring path MTU

On 1-Gbps and 10-Gbps ports in the mirroring path, you can reduce the number of dropped frames by enabling jumbo frames on all intermediate switches and routers. (The MTU on the switches covered by this manual is 9220 bytes for frames having an 802.1Q VLAN tag, and 9216 bytes for untagged frames.)

Table 33 Maximum frame sizes for mirroring

	Frame type configuration	Maximum frame size	VLAN tag	Frame mirrored to local port	Frame mirrored to remote port	
				Data	Data	IPv4 header
Untagged	Non-jumbo (default config.)	1518	0	1518	1464	54
	Jumbo[1] on all VLANs	9216	0	9216	9162	54
	Jumbo[1] On all but source VLAN	1518	0	n/a[2]	1464	54
Tagged	Non-jumbo	1522	4	1522	1468	54

Table 33 Maximum frame sizes for mirroring *(continued)*

	Frame type configuration	Maximum frame size	VLAN tag	Frame mirrored to local port	Frame mirrored to remote port	
				Data	Data	IPv4 header
	Jumbo[1] on all VLANs	9220	4	9218	9164	54
	Jumbo[1] On all but source VLAN	1522	4	n/a[2]	1468	54

[1] Jumbo frames are allowed on ports operating at or above 1 Gbps

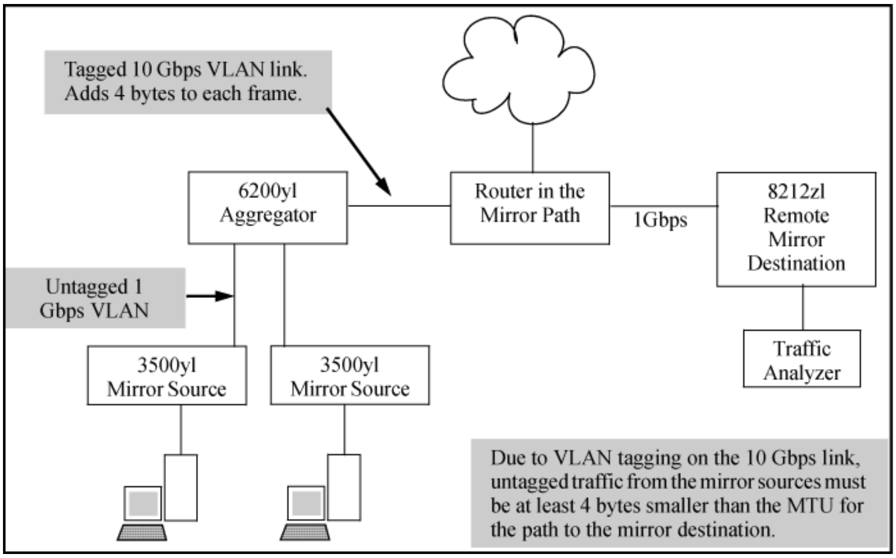
[2] For local mirroring, a non-jumbo configuration on the source VLAN dictates an MTU of 1518 bytes for untagged frames, and an MTU of 1522 for tagged frames, regardless of the jumbo configuration on any other VLANs on the switch.

Effect of downstream VLAN tagging on untagged, mirrored traffic

In a remote mirroring application, if mirrored traffic leaves the switch without 802.1Q VLAN tagging, but is forwarded through a downstream device that adds 802.1Q VLAN tags, the MTU for untagged mirrored frames leaving the source switch is reduced below the values shown in Table 33 (page 384).

For example, if the MTU on the path to the destination is 1522 bytes, untagged mirrored frames leaving the source switch cannot exceed 1518 bytes. Likewise, if the MTU on the path to the destination is 9220 bytes, untagged mirrored frames leaving the source switch cannot exceed 9216 bytes.

Figure 212 Effect of downstream VLAN tagging on the MTU for mirrored traffic


Tagged 10 Gbps VLAN link. Adds 4 bytes to each frame.
6200yl Aggregator
Router in the Mirror Path
1Gbps
8212zl Remote Mirror Destination
Untagged 1 Gbps VLAN
3500yl Mirror Source
3500yl Mirror Source
Traffic Analyzer
Due to VLAN tagging on the 10 Gbps link, untagged traffic from the mirror sources must be at least 4 bytes smaller than the MTU for the path to the mirror destination.

Operating notes for traffic mirroring

- **Mirroring dropped traffic**

  When an interface is configured to mirror traffic to a local or remote destination, packets are mirrored regardless of whether the traffic is dropped while on the interface. For example, if an ACL is configured on a VLAN with a `deny` ACE that eliminates packets from a Telnet application, the switch still mirrors the Telnet packets that are received on the interface and subsequently dropped.

- **Mirroring and spanning tree**

  Mirroring is performed regardless of the STP state of a port or trunk. This means, for example, that inbound traffic on a port blocked by STP can still be monitored for STP packets during the STP setup phase.

- **Tagged and untagged frames**

  For a frame entering or leaving the switch on a mirrored port, the mirrored copy retains the tagged or untagged state the original frame carried when it entered into or exited from the switch. (The tagged or untagged VLAN membership of ports in the path leading to the mirroring destination does not affect the tagged or untagged status of the mirrored copy itself.)

  Thus, if a tagged frame arrives on a mirrored port, the mirrored copy is also tagged, regardless of the status of ports in the destination path. If a frame exits from the switch on a mirrored port that is a tagged member of a VLAN, the mirrored copy is also tagged for the same reason.

  To prevent a VLAN tag from being added to the mirrored copy of an outbound packet sent to a mirroring destination, you must enter the `no-tag-added` parameter when you configure a port, trunk, or mesh interface to select mirrored traffic. For more information, see "Selecting all traffic on a port interface for mirroring according to traffic direction (CLI)" (page 347) and "Untagged mirrored packets" (page 373).

- **Effect of IGMP on mirroring**

  If both inbound and outbound mirroring is operating when IGMP is enabled on a VLAN, two copies of mirrored IGMP frames may appear at the mirroring destination.

- **Mirrored traffic not encrypted**

  Mirrored traffic undergoes IPv4 encapsulation, but mirrored encapsulated traffic is not encrypted.

- **IPv4 header added**

  The IPv4 encapsulation of mirrored traffic adds a 54-byte header to each mirrored frame. If a resulting frame exceeds the maximum MTU allowed in the network, it is dropped or truncated (according to the setting of the `[truncation]` parameter in the `mirror` command).

  To reduce the number of dropped frames, enable jumbo frames in the mirroring path, including all intermediate switches and/or routers. (The MTU on the switch is 9220 bytes, which includes 4 bytes for the 802.1Q VLAN tag.) For more information, see "Maximum supported frame size" (page 384). To configure the switch for jumbo frames, see Chapter 5.

- **Intercepted or injected traffic**

  The mirroring feature does not protect against either mirrored traffic being intercepted or traffic being injected into a mirrored stream by an intermediate host.

- **Inbound mirrored IPv4-encapsulated frames are not mirrored**

  The switch does not mirror IPv4-encapsulated mirrored frames that it receives on an interface. This prevents duplicate mirrored frames in configurations where the port connecting the switch to the network path for a mirroring destination is also a port whose inbound or outbound traffic is being mirrored.

  For example, if traffic leaving the switch through ports B5, B6, and B7 is being mirrored through port B7 to a network analyzer, the mirrored frames from traffic on ports B5 and B6 will not be mirrored a second time as they pass through port B7.

- **Switch operation as both destination and source**

  A switch configured as a remote destination switch can also be configured to mirror traffic to one of its own ports (local mirroring) or to a destination on another switch (remote mirroring).

- **Monitor command note**

  If session 1 is already configured with a destination, you can enter the `[no] vlan` *`vid`* `monitor` or `[no] interface` *`port`* `monitor` command without mirroring criteria and a mirror session number. In this case, the switch automatically configures or removes mirroring for inbound and outbound traffic from the specified VLAN or ports to the destination configured for session 1.

- **Loss of connectivity suspends remote mirroring**

  When a remote mirroring session is configured on a source switch, the switch sends an ARP request to the configured destination approximately every 60 seconds. If the source switch fails to receive the expected ARP response from the destination for the session, transmission of mirrored traffic in the session halts. However, because the source switch continues to send ARP requests for each configured remote session, link restoration or discovery of another path to the destination enables the source switch to resume transmitting the session's mirrored traffic after a successful ARP response cycle occurs.

  Note that if a link's connectivity is repeatedly interrupted ("link toggling"), little or no mirrored traffic may be allowed for sessions using that link. To verify the status of any mirroring session configured on the source switch, use the `show monitor` command.

Troubleshooting traffic mirroring

If mirrored traffic does not reach the configured remote destination (endpoint) switch or remote exit port, check the following configurations:

- In a remote mirroring session, the `mirror remote ip` command parameters configured on the source switch for source IP address, source UDP port, and destination IP address must be identical to the same parameters configured with the `mirror endpoint ip` command on the remote destination switch.
- The configured remote exit port must not be a member of a trunk or mesh.
- If the destination for mirrored traffic is on a different VLAN than the source, routing must be correctly configured along the path from the source to the destination.
- On the remote destination (endpoint) switch, the IP addresses of the remote exit port and the switch can belong to different VLANs.
- All links on the path from the source switch to the destination switch must be active.

△ **CAUTION:**
A mirroring exit port should be connected only to a network analyzer, IDS, or other network edge device that has no connection to other network resources. Configuring a mirroring exit port connection to a network can result in serious network performance problems, and is strongly discouraged by HP Switch Networking.

C Troubleshooting

Overview

This appendix addresses performance-related network problems that can be caused by topology, switch configuration, and the effects of other devices or their configurations on switch operation. (For switch-specific information on hardware problems indicated by LED behavior, cabling requirements, and other potential hardware-related problems, see the *Installation Guide* you received with the switch.)

NOTE: HP periodically places switch software updates on the HP Switch Networking website. HP Switch recommends that you check this website for software updates that may have fixed a problem you are experiencing.

For information on support and warranty provisions, see the Support and Warranty booklet shipped with the switch.

Table 34 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
`fault-finder link-flap sensitivity [ low | medium | high ] action [ warn | warn-and-disable ]`	Expands the functionality of the existing fault finder function to include a "link-flap" event and a new action of "warn-and-disable."	Sensitivity=Medium; Action=Warn	(page 407)	
`show logging [-a, -b, -r, -s, -t, -m, -p, -w, -i, -d] [ *option-str* ]`	Displays the log messages recorded since the last reboot in chronological order.		(page 423)	(page 424)
	Navigating in the Event Log			(page 425)
`clear logging`	Removes all entries from the event log display output.		(page 425)	
`[ no ] log-numbers`	Turns event numbering on and off.		(page 426)	
`show debug`	Displays the currently configured debug logging destinations and message types selected for debugging purposes.		(page 432)	
`[ no ] debug *debug-type*`	Configures the types of debug messages that the switch can send to configured debug destinations.		(page 435)	
`[ no ] debug *debug type* include [ ip ip-addr list | port *port-list* | vlan *vid-list* ]`	Enables or disables debug message filtering for a debug type.	Disabled	(page 439)	

Table 34 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
[no] debug destination [logging | session | buffer] logging	Enables (and disables) syslog messaging on a syslog server or to a CLI session for specified types of debug and Event Log messages.	Logging disabled	(page 440)	
[no] logging *syslog-ip-addr*	Enables or disables syslog messaging to the specified IP address.		(page 442)	
[no] logging *ip-addr* [udp 1024-49151 | tcp 1024-49151]	Allows the configuration of the UDP or TCP transport protocol for the transmission of logging messages to a syslog server.	Default ports: UDP port is 514 TCP port is 1470 Default Transport Protocol: UDP	(page 443)	
[no] logging facility *facility-name*	The logging facility specifies the destination subsystem used in a configured syslog server.		(page 443)	
logging *ip-addr* [control-descr *text_string*] no logging *ip-addr* [control-descr]	An optional user-friendly description that can be associated with a server IP address.		(page 444)	
logging priority-descr *text_string* no logging priority-descr	Provides a user-friendly description for the combined filter values of severity and system module.		(page 444)	
[no] logging severity [major | error | warning | info | debug]	Selects a set of Event Log messages according to their severity level and send them to a syslog server.	Debug	(page 445)	
[no] logging system-module *system-module*	Configures the switch to send all Event Log messages being logged from the specified system module to configured syslog servers.	all-pass	(page 445)	
ping [ip-address | hostname] [repetitions 1-10000] [timeout 1-60] [source [ip-address | vlan-id | loopback 0-7]] [data-size 0 -	Sends ICMP echo requests to determine if another device is alive.		(page 448)	

Table 34 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
65471] [data-fill 0-1024] [ip-option [record-route | loose-source-route | strict-source-route | include-timestamp | include-timestamp-and-address | include timestamp-from]] [tos 0-255] ping6 [ipv6-address | hostname] [repetitions 1-10000] [timeout 1-60] [source [ip-address | vlan-id | loopback 0-7]] [data-size 0 - 65471] [data-fill 0-1024]				
link *mac-address* [repetitions 1 - 999] [timeout 1 - 256] [vlan *vlan-id*]	Issues single or multiple link tests.	Repetitions: 1 Timeout: 5 seconds	(page 450)	
traceroute ip-address | hostname [maxttl 1-255] [minttl 1-255] [probes 1-5] [source [ip-address | source-vlan vid | loopback 0-7]] [dstport 1-34000] [srcport 1-34000] [ip-option [record-route | loose-source-route | strict-source-route | include-timestamp | include-timestamp-and-address | include timestamp-from]] [timeout 1-120]	Lists the IP address or hostname of each hop in the route, plus the time in microseconds for the traceroute packet reply to the switch for each hop.		(page 450)	
write terminal	Displays the running configuration.		(page 453)	

Table 34 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`show tech`	Displays a single output of switch operating and running-configuration data from several internal switch sources.		(page 453)	
`copy` *`source`* `show- tech`	Specifies the operational and configuration data from one or more source files to be displayed by the `show tech` command.		(page 456)	
`show boot-history`	Displays the crash information saved for each management module on the switch.		(page 457)	
`show history`	Displays the current command history.		(page 457)	
`show system-information`	Displays globally configured parameters and information on switch operation.		(page 457)	
`show version`	Displays the software version currently running on the switch and the flash image from which the switch booted.		(page 457)	
`show interfaces`	Displays information on the activity on all switch ports.		(page 457)	
`show interfaces-display`	Displays the same information as the `show interfaces` command and dynamically updates the output every three seconds.		(page 457)	
`show` [*`command option`* `include | exclude | begin`] `regular expression`	Uses matching pattern searches to display selected portions of the output from a `show` command.		(page 458)	
`alias`	Creates a shortcut alias name for commonly used commands and command options.		(page 460)	
`kill`	Terminates a currently running, remote troubleshooting session.		(page 460)	

Table 34 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`[ no ]page`	Toggles the paging mode for `show` commands between continuous listing and per-page listing.		(page 460)	
`repeat`	Repeatedly executes one or more commands so that you can see the results of multiple commands displayed over a period of time.		(page 460)	
`setup`	Displays the Switch Setup screen from the menu interface.		(page 460)	
`erase startup-configuration`	Deletes the startup-config file in flash so that the switch will reboot with its factory-default configuration.		(page 461)	(page 461)
	Recovering from an empty or corrupted flash state			(page 461)
`[ no ] ip dns server-address priority 1 - 3` *`ip-addr`*	Configures the access priority and IP address of a DNS server accessible to the switch.		(page 465)	
`[ no ] ip dns domain-name` *`domain-name-suffix`*	Configures the domain suffix that is automatically appended to the host name entered with a DNS-compatible command.		(page 465)	
`chassislocate [ blink | on | off ]`	Locates a switch by using the blue Locate LED on the front panel.		(page 468)	

Troubleshooting approaches

Use these approaches to diagnose switch problems:

- Check the HP website for software updates that may have solved your problem: **www.hp.com/Networking/support**
- Check the switch LEDs for indications of proper switch operation:
  - Each switch port has a Link LED that should light whenever an active network device is connected to the port.
  - Problems with the switch hardware and software are indicated by flashing the Fault and other switch LEDs.

    For a description of the LED behavior and information on using the LEDs for troubleshooting, see the *Installation Guide* shipped with the switch.

- Check the network topology/installation. For topology information, see the *Installation Guide* shipped with the switch.
- Check cables for damage, correct type, and proper connections. You should also use a cable tester to check your cables for compliance to the relevant IEEE 802.3 specification. For correct cable types and connector pin-outs, see the *Installation Guide* shipped with the switch.
- Use HP PCM+ to help isolate problems and recommend solutions.
- Use the Port Utilization Graph and Alert Log in the WebAgent included in the switch to help isolate problems. These tools are available through the WebAgent:
  - Alert log
  - Port Status and Port Counters screens
  - Diagnostic tools (Link test, Ping test, configuration file browser)
- For help in isolating problems, use the easy-to-access switch console built into the switch or Telnet to the switch console. For operating information on the Menu and CLI interfaces included in the console, see chapters 3 and 4. These tools are available through the switch console:
  - Status and Counters screens
  - Event Log
  - Diagnostics tools (Link test, Ping test, configuration file browser, and advanced user commands)

Browser or Telnet access problems

Cannot access the WebAgent

- Access may be disabled by the Web Agent Enabled parameter in the switch console. Check the setting on this parameter by selecting:

  2. Switch Configuration
  1. System Information

- The switch may not have the correct IP address, subnet mask, or gateway. Verify by connecting a console to the switch's Console port and selecting:

  2. Switch Configuration
  5. IP Configuration

  Note: If DHCP/Bootp is used to configure the switch, the IP addressing can be verified by selecting:

  1. Status and Counters...
  2. Switch Management Address Information

  Also check the DHCP/Bootp server configuration to verify correct IP addressing.

- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, see the documentation for the DHCP application that you are using.
- If one or more IP-authorized managers are configured, the switch allows inbound telnet access only to a device having an authorized IP address. For more information on IP Authorized managers, see the Access Security Guide for your switch.
- Java™ applets may not be running on the web browser. They are required for the switch WebAgent to operate correctly. Refer to the online Help on your web browser for how to run the Java applets.

Cannot Telnet into the switch console from a station on the network

- Off-subnet management stations can lose Telnet access if you enable routing without first configuring a static (default) route. That is, the switch uses the IP default gateway only while operating as a Layer 2 device. While routing is enabled on the switch, the IP default gateway is not used. You can avoid this problem by using the ip route command to configure a static (default) route before enabling routing. For more information, see chapter "IP Routing Features" in the *Multicast and Routing Guide* for your switch.
- Telnet access may be disabled by the `Inbound Telnet Enabled` parameter in the System Information screen of the menu interface:

  2. Switch Configuration
  1. System Information

- The switch may not have the correct IP address, subnet mask, or gateway. Verify by connecting a console to the switch's Console port and selecting:

  2. Switch Configuration
  5. IP Configuration

- If you are using DHCP to acquire the IP address for the switch, the IP address "lease time" may have expired so that the IP address has changed. For more information on how to "reserve" an IP address, see the documentation for the DHCP application that you are using.
- If one or more IP-authorized managers are configured, the switch allows inbound telnet access only to a device having an authorized IP address. For more information on IP Authorized managers, see the Access Security Guide for your switch.

Unusual network activity

Network activity that fails to meet accepted norms may indicate a hardware problem with one or more of the network components, possibly including the switch. Such problems can also be caused by a network loop or simply too much traffic for the network as it is currently designed and implemented. Unusual network activity is usually indicated by the LEDs on the front of the switch or measured with the switchconsole interface or with a network management tool such as HP PCM+. For information on using LEDs to identify unusual network activity, see the *Installation Guide* you received with the switch.

A topology loop can also cause excessive network activity. The Event Log "FFI" messages can be indicative of this type of problem.

General problems

The network runs slow; processes fail; users cannot access servers or other devices

Broadcast storms may be occurring in the network. These may be caused by redundant links between nodes.

- If you are configuring a port trunk, finish configuring the ports in the trunk before connecting the related cables. Otherwise you may inadvertently create a number of redundant links (that is, topology loops) that will cause broadcast storms.
- Turn on STP to block redundant links
- Check for FFI messages in the Event Log.

Duplicate IP addresses

This is indicated by this Event Log message:

```
ip: Invalid ARP source: IP address on IP address
```

where both instances of *`IP address`* are the same address, indicating that the switch's IP address has been duplicated somewhere on the network.

Duplicate IP addresses in a DHCP network

If you use a DHCP server to assign IP addresses in your network, and you find a device with a valid IP address that does not appear to communicate properly with the server or other devices, a duplicate IP address may have been issued by the server. This can occur if a client has not released a DHCP-assigned IP address after the intended expiration time and the server "leases" the address to another device. This can also happen, for example, if the server is first configured to issue IP addresses with an unlimited duration, and then is subsequently configured to issue IP addresses that will expire after a limited duration. One solution is to configure "reservations" in the DHCP server for specific IP addresses to be assigned to devices having specific MAC addresses. For more information, see the documentation for the DHCP server.

One indication of a duplicate IP address in a DHCP network is this Event Log message:

```
ip: Invalid ARP source: IP-address  on IP-address
```

where both instances of *`IP-address`* are the same address, indicating that the IP address has been duplicated somewhere on the network.

The switch has been configured for DHCP/Bootp operation, but has not received a DHCP or Bootp reply

When the switch is first configured for DHCP/Bootp operation, or if it is rebooted with this configuration, it immediately begins sending request packets on the network. If the switch does not receive a reply to its DHCP/Bootp requests, it continues to periodically send request packets, but with decreasing frequency. Thus, if a DHCP or Bootp server is not available or accessible to the switch when DHCP/Bootp is first configured, the switch may not immediately receive the desired configuration.

After verifying that the server has become accessible to the switch, reboot the switch to re-start the process.

802.1Q Prioritization problems

Ports configured for non-default prioritization (level 1 to 7) are not performing the specified action

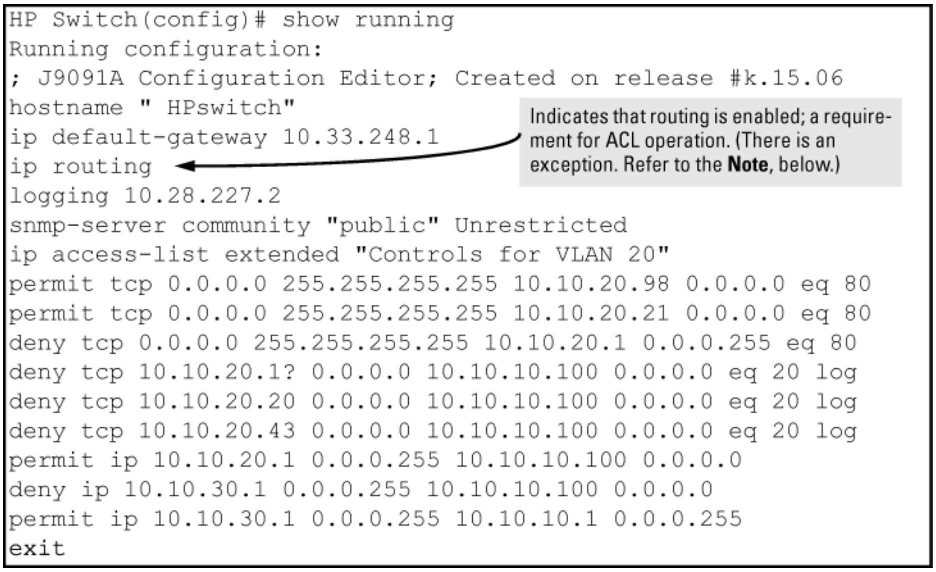
If the ports were placed in a trunk group after being configured for nondefault prioritization, the priority setting was automatically reset to zero (the default). Ports in a trunk group operate only at the default priority setting.

Addressing ACL problems

ACLs are properly configured and assigned to VLANs, but the switch is not using the ACLs to filter IP layer 3 packets

1. The switch may be running with IP routing disabled. To ensure that IP routing is enabled, execute `show running` and look for the IP routing statement in the resulting listing. For example:

   Figure 213 Indication that routing is enabled

   ```
   HP Switch(config)# show running
   Running configuration:
   ; J9091A Configuration Editor; Created on release #k.15.06
   hostname " HPswitch"
   ip default-gateway 10.33.248.1
   ip routing
   logging 10.28.227.2
   snmp-server community "public" Unrestricted
   ip access-list extended "Controls for VLAN 20"
   permit tcp 0.0.0.0 255.255.255.255 10.10.20.98 0.0.0.0 eq 80
   permit tcp 0.0.0.0 255.255.255.255 10.10.20.21 0.0.0.0 eq 80
   deny tcp 0.0.0.0 255.255.255.255 10.10.20.1 0.0.0.255 eq 80
   deny tcp 10.10.20.1? 0.0.0.0 10.10.10.100 0.0.0.0 eq 20 log
   deny tcp 10.10.20.20 0.0.0.0 10.10.10.100 0.0.0.0 eq 20 log
   deny tcp 10.10.20.43 0.0.0.0 10.10.10.100 0.0.0.0 eq 20 log
   permit ip 10.10.20.1 0.0.0.255 10.10.10.100 0.0.0.0
   deny ip 10.10.30.1 0.0.0.255 10.10.10.100 0.0.0.0
   permit ip 10.10.30.1 0.0.0.255 10.10.10.1 0.0.0.255
   exit
   ```

   Indicates that routing is enabled; a requirement for ACL operation. (There is an exception. Refer to the **Note**, below.)

   NOTE: If an ACL assigned to a VLAN includes an ACE referencing an IP address on the switch itself as a packet source or destination, the ACE screens traffic to or from this switch address regardless of whether IP routing is enabled. This is a security measure designed to help protect the switch from unauthorized management access.

   If you need to configure IP routing, execute the `ip routing` command.

2. ACL filtering on the switches applies only to routed packets and packets having a destination IP address (DA) on the switch itself.

   Also, the switch applies assigned ACLs only at the point where traffic enters or leaves the switch on a VLAN. Ensure that you have correctly applied your ACLs ("in" and/or "out") to the appropriate VLANs.

The switch does not allow management access from a device on the same VLAN

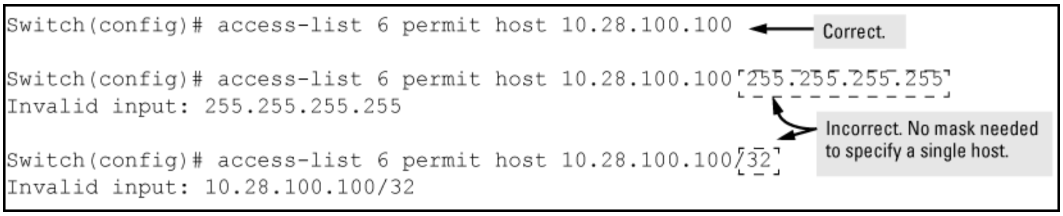
The implicit `deny any` function that the switch automatically applies as the last entry in any ACL always blocks packets having the same DA as the switch's IP address on the same VLAN. That is, bridged packets with the switch itself as the destination are blocked as a security measure.

To preempt this action, edit the ACL to include an ACE that permits access to the switch's DA on that VLAN from the management device.

Error (Invalid input) when entering an IP address

When using the "host" option in the command syntax, ensure that you are not including a mask in either dotted decimal or CIDR format. Using the "host" option implies a specific host device and therefore does not permit any mask entry.

Figure 214 Examples of correctly and incorrectly specifying a single host



```
Switch(config)# access-list 6 permit host 10.28.100.100

Switch(config)# access-list 6 permit host 10.28.100.100 255.255.255.255
Invalid input: 255.255.255.255

Switch(config)# access-list 6 permit host 10.28.100.100/32
Invalid input: 10.28.100.100/32
```

Correct.

Incorrect. No mask needed to specify a single host.

Apparent failure to log all "deny" matches

Where the `log` statement is included in multiple ACEs configured with a "deny" option, a large volume of "deny" matches generating logging messages in a short period of time can impact switch performance. If it appears that the switch is not consistently logging all "deny" matches, try reducing the number of logging actions by removing the `log` statement from some ACEs configured with the "deny" action.

The switch does not allow any routed access from a specific host, group of hosts, or subnet

The implicit `deny any` function that the switch automatically applies as the last entry in any ACL may be blocking all access by devices not specifically permitted by an entry in an ACL affecting those sources. If you are using the ACL to block specific hosts, a group of hosts, or a subnet, but want to allow any access not specifically permitted, insert `permit any` as the last explicit entry in the ACL.

The switch is not performing routing functions on a VLAN

Two possible causes of this problem are:

- Routing is not enabled. If `show running` indicates that routing is not enabled, use the `ip routing` command to enable routing.
- An ACL may be blocking access to the VLAN (on a switch covered in this guide). Ensure that the switch's IP address on the VLAN is not blocked by one of the ACE entries in an ACL applied to that VLAN. A common mistake is to either not explicitly permit the switch's IP address as a DA or to use a wildcard ACL mask in a `deny` statement that happens to include the switch's IP address. For an example of this problem, see section "General ACL Operating Notes" in the "Access Control Lists (ACLs)" chapter of the latest *Access Security Guide* for your switch.

Routing through a gateway on the switch fails

Configuring a "deny" ACE that includes a gateway address can block traffic attempting to use the gateway as a next-hop.

Examples

Remote gateway case

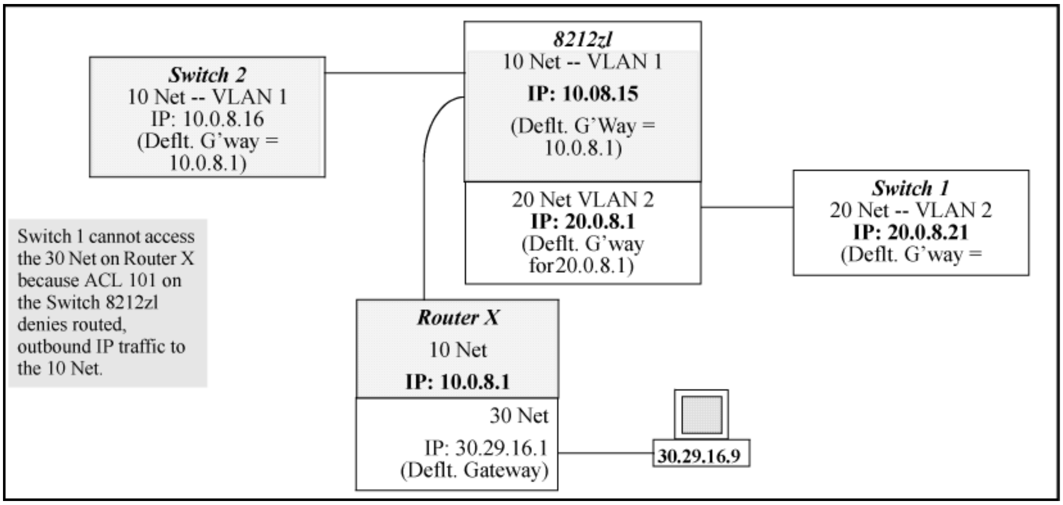
Configuring ACL "101" (Example 64 (page 398)) and applying it outbound on VLAN 1 in Figure 215 (page 398) includes the router gateway (10.0.8.1) needed by devices on other networks. This can prevent the switch from sending ARP and other routing messages to the gateway router to support traffic from authorized remote networks.

Example 64 ACE blocking an entire subnet

In Figure 215 (page 398), this ACE (see data in bold below) denies access to the 10 Net's 10.0.8.1 router gateway needed by the 20 Net (Subnet mask is 255.255.255.0).

```
HP Switch(config)# access-list config

ip access-list extended "101"
  deny ip 0.0.0.0 255.255.255.255 10.0.8.30 0.0.0.255
  permit ip 0.0.0.0 255.255.255.255 0.0.0.00 255.255.255.255
  exit
```

Figure 215 Inadvertently blocking a gateway



To avoid inadvertently blocking the remote gateway for authorized traffic from another network (such as the 20 Net in this example):

1. Configure an ACE that specifically permits authorized traffic from the remote network.
2. Configure narrowly defined ACEs to block unwanted IP traffic that would otherwise use the gateway; such ACEs might deny traffic for a particular application, particular hosts, or an entire subnet.
3. Configure a "permit any" ACE to specifically allow any IP traffic to move through the gateway.

Local gateway case

If you use the switch as a gateway for traffic you want routed between subnets, use these general steps to avoid blocking the gateway for authorized applications:

1. Configure gateway security first for routing with specific permit and deny statements.
2. Permit authorized traffic.
3. Deny any unauthorized traffic that you have not already denied in step 1 (page 398).

IGMP-related problems

IP multicast (IGMP) traffic that is directed by IGMP does not reach IGMP hosts or a multicast router connected to a port

IGMP must be enabled on the switch and the affected port must be configured for "Auto" or "Forward" operation.

IP multicast traffic floods out all ports; IGMP does not appear to filter traffic

The IGMP feature does not operate if the switch or VLAN does not have an IP address configured manually or obtained through DHCP/Bootp. To verify whether an IP address is configured for the switch or VLAN, do one of the following:

- **Try using the WebAgent**: If you can access the WebAgent, then an IP address is configured.
- **Try to telnet to the switch console**: If you can Telnet to the switch, an IP address is configured.
- **Use the switch console interface**: From the Main Menu, check the Management Address Information screen by clicking on:
  1. Status and Counters
  2. Switch Management Address Information

LACP-related problems

Unable to enable LACP on a port with the `interface` *`port-number`* `lacp` command. In this case, the switch displays the following message

Operation is not allowed for a trunked port.

You cannot enable LACP on a port while it is configured as a static `Trunk` port. To enable LACP on a static-trunked port:

1. Use the `no trunk` *`port-number`* command to disable the static trunk assignment.
2. Execute `interface` *`port-number`* `lacp`.

△ **CAUTION:** Removing a port from a trunk without first disabling the port can create a traffic loop that can slow down or halt your network. Before removing a port from a trunk, HP recommends that you either disable the port or disconnect it from the LAN.

Mesh-related problems

Traffic on a dynamic VLAN does not get through the switch mesh

GVRP enables dynamic VLANs. Ensure that all switches in the mesh have GVRP enabled.

Port-based access control (802.1X)-related problems

NOTE: To list the 802.1X port-access Event Log messages stored on the switch, use `show log 802`.

See also "Radius-related problems" (page 401).

The switch does not receive a response to RADIUS authentication requests

In this case, the switch attempts authentication using the secondary method configured for the type of access you are using (console, Telnet, or SSH).

There can be several reasons for not receiving a response to an authentication request. Do the following:

- Use `ping` to ensure that the switch has access to the configured RADIUS servers.
- Verify that the switch is using the correct encryption key (RADIUS secret key) for each server.
- Verify that the switch has the correct IP address for each RADIUS server.
- Ensure that the `radius-server timeout` period is long enough for network conditions.

The switch does not authenticate a client even though the RADIUS server is properly configured and providing a response to the authentication request

If the RADIUS server configuration for authenticating the client includes a VLAN assignment, ensure that the VLAN exists as a static VLAN on the switch. See "How 802.1X Authentication Affects VLAN Operation" in the *Access Security Guide* for your switch.

During RADIUS-authenticated client sessions, access to a VLAN on the port used for the client sessions is lost

If the affected VLAN is configured as untagged on the port, it may be temporarily blocked on that port during an 802.1X session. This is because the switch has temporarily assigned another VLAN as untagged on the port to support the client access, as specified in the response from the RADIUS server. See "How 802.1X Authentication Affects VLAN Operation" in the *Access Security Guide* for your switch.

The switch appears to be properly configured as a supplicant, but cannot gain access to the intended authenticator port on the switch to which it is connected

If `aaa authentication port-access` is configured for Local, ensure that you have entered the local *login* (operator-level) username and password of the authenticator switch into the `identity` and `secret` parameters of the supplicant configuration. If instead, you enter the enable (manager-level) username and password, access will be denied.

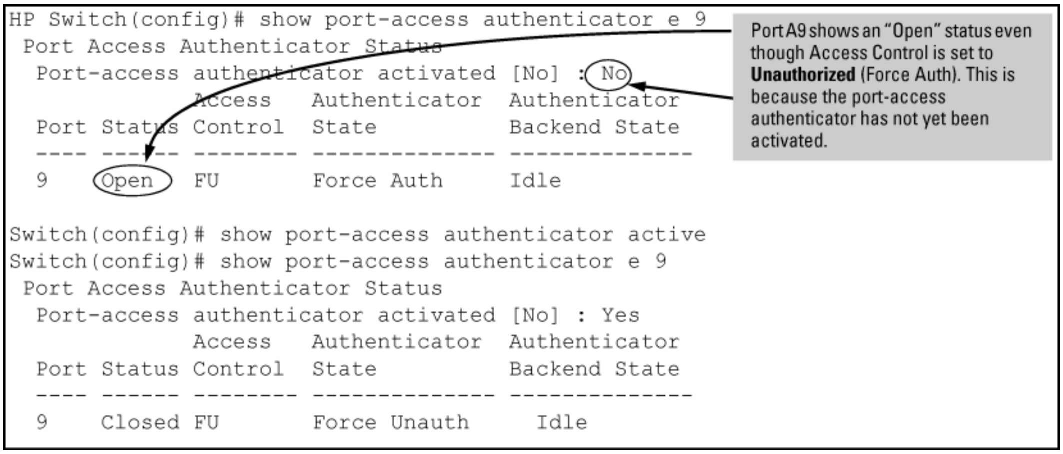
The supplicant statistics listing shows multiple ports with the same authenticator MAC address

The link to the authenticator may have been moved from one port to another without the supplicant statistics having been cleared from the first port. See "Note on Supplicant Statistics" in the chapter on Port-Based and User-Based Access Control in the *Access Security Guide* for your switch.

The `show port-access authenticator` *`port-list`* command shows one or more ports remain open after they have been configured with `control unauthorized`

802.1X is not active on the switch. After you execute `aaa port-access authenticator active`, all ports configured with `control unauthorized` should be listed as `Closed`.

Figure 216 Authenticator ports remain "open" until activated



```
HP Switch(config)# show port-access authenticator e 9
 Port Access Authenticator Status
  Port-access authenticator activated [No] : No
                 Access   Authenticator  Authenticator
  Port Status Control  State          Backend State
  ---- ------ -------- -------------- --------------
  9    Open   FU       Force Auth     Idle

Switch(config)# show port-access authenticator active
Switch(config)# show port-access authenticator e 9
 Port Access Authenticator Status
  Port-access authenticator activated [No] : Yes
                 Access   Authenticator  Authenticator
  Port Status Control  State          Backend State
  ---- ------ -------- -------------- --------------
  9    Closed FU       Force Unauth     Idle
```

Port A9 shows an "Open" status even though Access Control is set to **Unauthorized** (Force Auth). This is because the port-access authenticator has not yet been activated.

RADIUS server fails to respond to a request for service, even though the server's IP address is correctly configured in the switch

Use `show radius` to verify that the encryption key (RADIUS secret key) the switch is using is correct for the server being contacted. If the switch has only a global key configured, it either must match the server key or you must configure a server-specific key. If the switch already has a server-specific key assigned to the server's IP address, it overrides the global key and must match the server key.

Figure 217 Displaying encryption keys

```
HP Switch(config)# show radius
 Status and Counters - General RADIUS Information
  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key : My-Global-Key
  Dynamic Authorization UDP Port : 3799

                  Auth Acct DM/ Time
  Server IP Addr  Port Port CoA Window Encryption Key
  --------------- ---- ---- --- ------ ---------------
  10.33.18.119    1812 1813            119-only-key
```

Also, ensure that the switch port used to access the RADIUS server is not blocked by an 802.1X configuration on that port. For example, `show port-access authenticator` *`port-list`* gives you the status for the specified ports. Also, ensure that other factors, such as port security or any 802.1X configuration on the RADIUS server are not blocking the link.

The authorized MAC address on a port that is configured for both 802.1X and port security either changes or is re-acquired after execution of aaa `port-access authenticator` *`port-list`* `initialize`

If the port is force-authorized with `aaa port-access authenticator` *`port-list`* `control authorized` command and port security is enabled on the port, then executing `initialize` causes the port to clear the learned address and learn a new address from the first packet it receives after you execute `initialize`.

A trunked port configured for 802.1X is blocked

If you are using RADIUS authentication and the RADIUS server specifies a VLAN for the port, the switch allows authentication, but blocks the port. To eliminate this problem, either remove the port from the trunk or reconfigure the RADIUS server to avoid specifying a VLAN.

QoS-related problems

Loss of communication when using VLAN-tagged traffic

If you cannot communicate with a device in a tagged VLAN environment, ensure that the device either supports VLAN tagged traffic or is connected to a VLAN port that is configured as `Untagged`.

Radius-related problems

The switch does not receive a response to RADIUS authentication requests

In this case, the switch attempts authentication using the secondary method configured for the type of access you are using (console, Telnet, or SSH).

There can be several reasons for not receiving a response to an authentication request. Do the following:

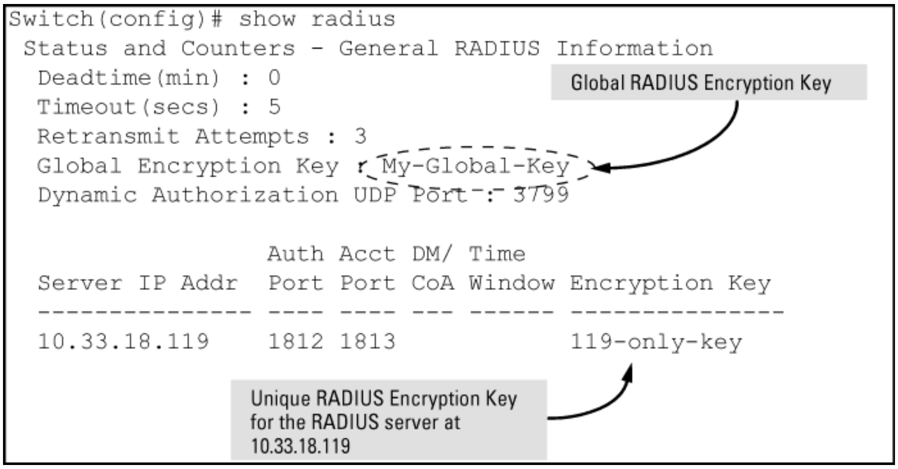
- Use `ping` to ensure that the switch has access to the configured RADIUS server.
- Verify that the switch is using the correct encryption key for the designated server.
- Verify that the switch has the correct IP address for the RADIUS server.
- Ensure that the `radius-server timeout` period is long enough for network conditions.
- Verify that the switch is using the same UDP port number as the server.

NOTE: Because of an inconsistency between the Windows XP 802.1x supplicant timeout value and the switch default timeout value, which is 5, when adding a backup RADIUS server, set the switch radius-server timeout value to 4. Otherwise, the switch may not failover properly to the backup RADIUS server.

RADIUS server fails to respond to a request for service, even though the server's IP address is correctly configured in the switch

Use `show radius` to verify that the encryption key the switch is using is correct for the server being contacted. If the switch has only a global key configured, it either must match the server key or you must configure a server-specific key. If the switch already has a server-specific key assigned to the server's IP address, it overrides the global key and must match the server key.

Figure 218 Examples of global and unique encryption keys



```
Switch(config)# show radius
 Status and Counters - General RADIUS Information
  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key : My-Global-Key
  Dynamic Authorization UDP Port : 3799

                  Auth Acct DM/ Time
  Server IP Addr  Port Port CoA Window Encryption Key
  --------------- ---- ---- --- ------ ---------------
  10.33.18.119    1812 1813            119-only-key
```

Global RADIUS Encryption Key
Unique RADIUS Encryption Key for the RADIUS server at 10.33.18.119

MSTP and fast-uplink problems

△ **CAUTION:** If you enable MSTP, HP recommends that you leave the remainder of the MSTP parameter settings at their default values until you have had an opportunity to evaluate MSTP performance in your network. Because incorrect MSTP settings can adversely affect network performance, you should avoid making changes without having a strong understanding of how MSTP operates. To learn the details of MSTP operation, see the IEEE802.1s standard.

Broadcast storms appearing in the network

This can occur when there are physical loops (redundant links) in the topology. Where this exists, you should enable MSTP on all bridging devices in the topology to detect the loop.

STP blocks a link in a VLAN even though there are no redundant links in that VLAN

In 802.1Q-compliant switches, MSTP blocks redundant physical links even if they are in separate VLANs. A solution is to use only one, multiple-VLAN (tagged) link between the devices. Also, if ports are available, you can improve the bandwidth in this situation by using a port trunk. See "Spanning Tree Operation with VLANs" in chapter "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.

Fast-uplink troubleshooting

Some of the problems that can result from incorrect use of fast-uplink MSTP include temporary loops and generation of duplicate packets.

Problem sources can include:

- Fast-uplink is configured on a switch that is the MSTP root device.
- Either the `Hello Time` or the `Max Age` setting (or both) is too long on one or more switches. Return the `Hello Time` and `Max Age` settings to their default values (2 seconds and 20 seconds, respectively, on a switch).
- A "downlink" port is connected to a switch that is further away (in hop count) from the root device than the switch port on which fast-uplink MSTP is configured.
- Two edge switches are directly linked to each other with a fast-uplink (Mode = `Uplink`) connection.

- Fast uplink is configured on both ends of a link.
- A switch serving as a backup MSTP root switch has ports configured for fast-uplink MSTP and has become the root device because of a failure in the original root device.

SSH-related problems

Switch access refused to a client

Even though you have placed the client's public key in a text file and copied the file (using the `copy tftp pub-key-file` command) into the switch, the switch refuses to allow the client to have access. If the source SSH client is an SSHv2 application, the public key may be in the PEM format, which the switch (SSHv1) does not interpret. Check the SSH client application for a utility that can convert the PEM-formatted key into an ASCII-formatted key.

Executing IP SSH does not enable SSH on the switch

The switch does not have a host key. Verify by executing `show ip host-public-key`. If you see the message

```
ssh cannot be enabled until a host key is configured (use 'crypto'
 command).
```

you need to generate an SSH key pair for the switch. To do so, execute `crypto key generate` (see "2. Generating the Switch's Public and Private Key Pair" in the SSH chapter of the *Access Security Guide* for your switch.)

Switch does not detect a client's public key that does appear in the switch's public key file (`show ip client-public-key`)

The client's public key entry in the public key file may be preceded by another entry that does not terminate with a new line (CR). In this case, the switch interprets the next sequential key entry as simply a comment attached to the preceding key entry. Where a public key file has more than one entry, ensure that all entries terminate with a new line (CR). While this is optional for the last entry in the file, not adding a new line to the last entry creates an error potential if you either add another key to the file at a later time or change the order of the keys in the file.

An attempt to copy a client public-key file into the switch has failed and the switch lists one of the following messages

```
Download failed: overlength key in key file.
Download failed: too many keys in key file.
Download failed: one or more keys is not a valid RSA public key.
```

The public key file you are trying to download has one of the following problems:

- A key in the file is too long. The maximum key length is 1024 characters, including spaces. This could also mean that two or more keys are merged together instead of being separated by a CRLF.
- There are more than ten public keys in the key file.
- One or more keys in the file is corrupted or is not a valid rsa public key.

Client ceases to respond ("hangs") during connection phase.

The switch does not support data compression in an SSH session. Clients often have compression turned on by default, but then disable it during the negotiation phase. A client that does not recognize the compression-request FAILURE response may fail when attempting to connect. Ensure that compression is turned *off* before attempting a connection to prevent this problem.

TACACS-related problems

Event Log

When troubleshooting TACACS+ operation, check the switch's Event Log for indications of problem areas.

All users are locked out of access to the switch

If the switch is functioning properly, but no username/password pairs result in console or Telnet access to the switch, the problem may be caused by how the TACACS+ server and/or the switch are configured. Use one of the following methods to recover:

- Access the TACACS+ server application and adjust or remove the configuration parameters controlling access to the switch.
- If the above method does not work, try eliminating configuration changes in the switch that have not been saved to flash (boot-up configuration) by causing the switch to reboot from the boot-up configuration (which includes only the configuration changes made prior to the last `write memory` command.) If you did not use `write memory` to save the authentication configuration to flash, pressing the `Reset` button or cycling the power reboots the switch with the boot-up configuration.
- Disconnect the switch from network access to any TACACS+ servers and then log in to the switch using either Telnet or direct console port access. Because the switch cannot access a TACACS+ server, it defaults to local authentication. You can then use the switch's local Operator or Manager username/password pair to log on.
- As a last resort, use the `Clear/Reset` button combination to reset the switch to its factory default boot-up configuration. Taking this step means you will have to reconfigure the switch to return it to operation in your network.

No communication between the switch and the TACACS+ server application

If the switch can access the server device (that is, it can `ping` the server), a configuration error may be the problem. Some possibilities include:

- The server IP address configured with the switch's `tacacs-server host` command may not be correct. (Use the switch's `show tacacs-server` command to list the TACACS+ server IP address.)
- The encryption key configured in the server does not match the encryption key configured in the switch (by using the `tacacs-server key` command). Verify the key in the server and compare it to the key configured in the switch. (Use `show tacacs-server` to list the global key. Use `show config` or `show config running` to list any server-specific keys.)
- The accessible TACACS+ servers are not configured to provide service to the switch.

Access is denied even though the username/password pair is correct

Some reasons for denial include the following parameters controlled by your TACACS+ server application:

- The account has expired.
- The access attempt is through a port that is not allowed for the account.
- The time quota for the account has been exhausted.
- The time credit for the account has expired.
- The access attempt is outside of the time frame allowed for the account.
- The allowed number of concurrent logins for the account has been exceeded.

For more help, see the documentation provided with your TACACS+ server application.

Unknown users allowed to login to the switch

Your TACACS+ application may be configured to allow access to unknown users by assigning them the privileges included in a *default user* profile. See the documentation provided with your TACACS+ server application.

System allows fewer login attempts than specified in the switch configuration

Your TACACS+ server application may be configured to allow fewer login attempts than you have configured in the switch with the `aaa authentication num-attempts` command.

TimeP, SNTP, or Gateway problems

The switch cannot find the time server or the configured gateway

TimeP, SNTP, and Gateway access are through the primary VLAN, which in the default configuration is the DEFAULT_VLAN. If the primary VLAN has been moved to another VLAN, it may be disabled or does not have ports assigned to it.

VLAN-related problems

Monitor port

When using the monitor port in a multiple-VLAN environment, the switch handles broadcast, multicast, and unicast traffic output from the monitor port as follows:

- If the monitor port is configured for tagged VLAN operation on the same VLAN as the traffic from monitored ports, the traffic output from the monitor port carries the same VLAN tag.
- If the monitor port is configured for untagged VLAN operation on the same VLAN as the traffic from the monitored ports, the traffic output from the monitor port is untagged.
- If the monitor port is not a member of the same VLAN as the traffic from the monitored ports, traffic from the monitored ports does not go out the monitor port.

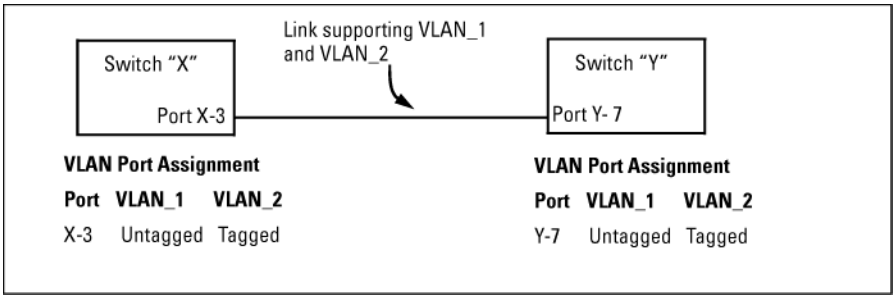
None of the devices assigned to one or more VLANs on an 802.1Q-compliant switch are being recognized

If multiple VLANs are being used on ports connecting 802.1Q-compliant devices, inconsistent VLAN IDs may have been assigned to one or more VLANs. For a given VLAN, the same VLAN ID must be used on all connected 802.1Q-compliant devices.

Link configured for multiple VLANs does not support traffic for one or more VLANs.

One or more VLANs may not be properly configured as "Tagged" or "Untagged." A VLAN assigned to a port connecting two 802.1Q-compliant devices must be configured the same on both ports. For example, VLAN_1 and VLAN_2 use the same link between switch "X" and switch "Y," as shown in Figure 219 (page 406).

Figure 219 Example of correct VLAN port assignments on a link



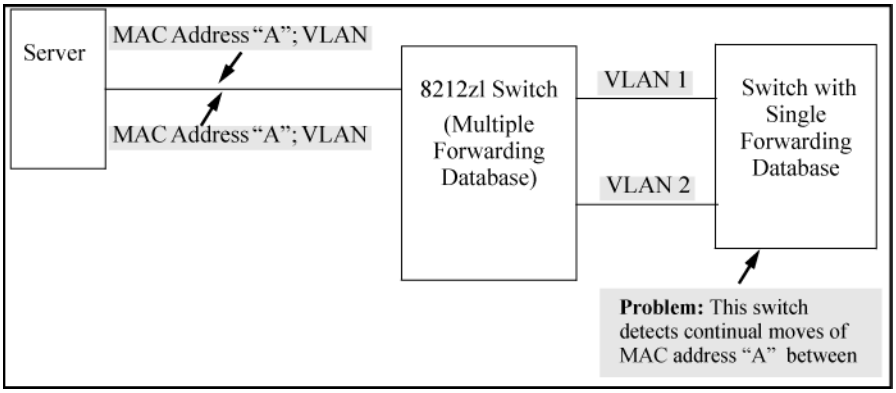
- If VLAN_1 (VID=1) is configured as "Untagged" on port 3 on switch "X," it must also be configured as "Untagged" on port 7 on switch "Y." Make sure that the VLAN ID (VID) is the same on both switches.
- Similarly, if VLAN_2 (VID=2) is configured as "Tagged" on the link port on switch "A," it must also be configured as "Tagged" on the link port on switch "B." Make sure that the VLAN ID (VID) is the same on both switches.

Duplicate MAC addresses across VLANs

The switches operate with multiple forwarding databases. Thus, duplicate MAC addresses occurring on different VLANs can appear where a device having one MAC address is a member of more than one 802.1Q VLAN, and the switch port to which the device is linked is using VLANs (instead of MSTP or trunking) to establish redundant links to another switch. If the other device sends traffic over multiple VLANs, its MAC address consistently appears in multiple VLANs on the switch port to which it is linked.

Be aware that attempting to create redundant paths through the use of VLANs causes problems with some switches. One symptom is that a duplicate MAC address appears in the Port Address Table of one port and then later appears on another port. While the switches have multiple forwarding databases and thus do not have this problem, some switches with a single forwarding database for all VLANs may produce the impression that a connected device is moving among ports because packets with the same MAC address but different VLANs are received on different ports. You can avoid this problem by creating redundant paths using port trunks or spanning tree.

Figure 220 Example of duplicate MAC address


Server
MAC Address "A"; VLAN
MAC Address "A"; VLAN
8212zl Switch (Multiple Forwarding Database)
VLAN 1
VLAN 2
Switch with Single Forwarding Database
Problem: This switch detects continual moves of MAC address "A" between

Fan failure

When two or more fans fail, a two-minute timer starts. After two minutes, the switch is powered down and must be rebooted to restart it. This protects the switch from possible overheating.

HP recommends that you replace a failed fan tray assembly within one minute of removing it.

Mitigating flapping transceivers

In traditional HP switches, the state of a link is driven directly by the reported state of the port, which is required for rapid detection of link faults. However, the consequence of this is that a marginal transceiver, optical, or wire cabling, one that "flaps" up and down several times per second, can cause STP and other protocols to react poorly, resulting in a network outage. The link-flap option expands the functionality of the existing fault finder function to include a "link-flap" event and a new action of "warn-and-disable." Together, these additions allow the errant condition to be detected, and the port in question can be optionally disabled.

Syntax:

```
fault-finder link-flap sensitivity  low | medium | high
action[ warn | warn-and-disable ]
```

Default settings: Sensitivity=Medium; Action = Warn

Sensitivity thresholds are static. In a 10-second window, if more than the threshold number of link state transitions (up or down) are detected, the event is triggered. The 10-second window is statically determined, that is, the counters are reset every 10 seconds, as opposed to being a sliding window. The counters are polled twice per second (every 500 milliseconds), and the event is triggered if the sensitivity threshold is crossed at that time.

The sensitivity thresholds are:

High	3 transitions in 10 seconds
Medium	6 transitions in 10 seconds
Low	10 transitions in 10 seconds

Configuring the link-flap event and corresponding action applies to all ports and port types (it is a global setting per FFI event type). Note that normal link transition protocols may prevent link state changes from occurring fast enough to trigger the event for some port types, configurations, and sensitivity settings.

When the link-flap threshold is met for a port configured for `warn` (for example,`fault-finder link-flap sensitivity medium action warn`), the following message is seen in the switch event log.

```
02672 FFI: port number-Excessive link state transitions
```

When the link-flap threshold is met for a port configured for warn-and-disable (for example, `fault-finder linkflap sensitivity medium action warn-and-disable`), the following messages are seen in the switch event log.

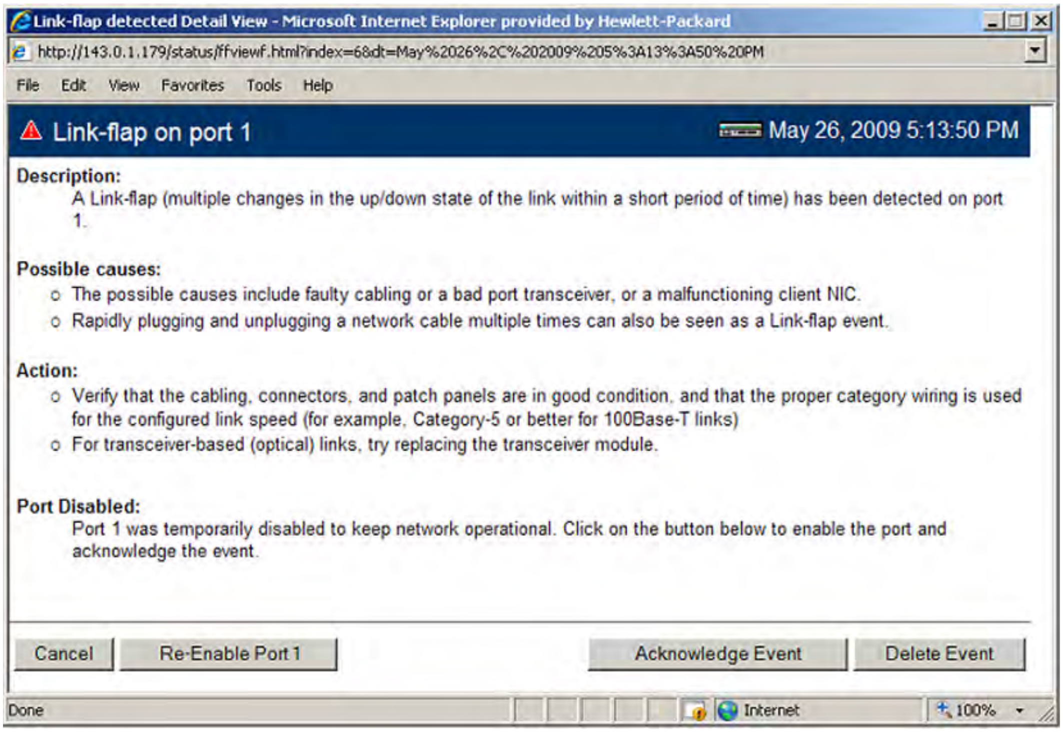
```
02672 FFI: port number-Excessive link state transitions
02673 FFI: port number-Port disabled by Fault-finder.
02674 FFI: port number-Administrator action required to re-enable.
```

The warn-and-disable action is available for all fault-finder events on an individual basis. It may be used, for example, to disable a port when excessive broadcasts are received. Because the fault-generated disabling of a port requires operator intervention to re-enable the port, such configuration should be used with care. For example, link-flap-initiated disablement is not desired on ports that are at the client edge of the network, because link state changes there are frequent and expected.

HP does not recommend automatic disabling of a port at the core or distribution layers when excessive broadcasts are detected, because of the potential to disable large parts of the network that may be uninvolved and for the opportunity to create a denial-of-service attack.

Within the Web Management interface, double-clicking an event on a port that was configured with warn-and-disable and that has met the threshold to trigger the disable action brings up a dialog box with the event details, as shown in Figure 221 (page 408). The event dialog box now contains a button at the bottom of the page, which can be used to re-enable the disabled port. The button remains, even if the port has already been brought up through a prior exercise of it, or if the port was re-enabled via some other interface (for example, the command line). Re-enabling an already enabled port has no effect. The button to acknowledge the event remains unchanged.

Figure 221 Link-flap on port 1 event detail dialog box


Link-flap detected Detail View - Microsoft Internet Explorer provided by Hewlett-Packard
http://143.0.1.179/status/ffviewf.html?index=6&dt=May%2026%2C%202009%205%3A13%3A50%20PM
File
Edit
View
Favorites
Tools
Help
Cancel
Re-Enable Port 1
Acknowledge Event
Delete Event
Done
Internet
100%

⚠ Link-flap on port 1 May 26, 2009 5:13:50 PM

Description:
A Link-flap (multiple changes in the up/down state of the link within a short period of time) has been detected on port 1.

Possible causes:

- The possible causes include faulty cabling or a bad port transceiver, or a malfunctioning client NIC.
- Rapidly plugging and unplugging a network cable multiple times can also be seen as a Link-flap event.

Action:

- Verify that the cabling, connectors, and patch panels are in good condition, and that the proper category wiring is used for the configured link speed (for example, Category-5 or better for 100Base-T links)
- For transceiver-based (optical) links, try replacing the transceiver module.

Port Disabled:
Port 1 was temporarily disabled to keep network operational. Click on the button below to enable the port and acknowledge the event.

Viewing transceiver information

This features provides the ability to view diagnostic monitoring information for transceivers with Diagnostic Optical Monitoring (DOM) support. The following transceivers are supported:

Product #	Description
J8436A	10GbE X2–SC SR Optic
J8437A	10GbE X2–SC LR Optic
J4858A	Gigabit-SX-LC Mini-GBIC
J4858B	Gigabit-SX-LC Mini-GBIC
J4858C[1]	Gigabit-SX-LC Mini-GBIC

[1] The J4858C transceivers that have the letters “VM” in their serial numbers do not support DOM.

Viewing information about transceivers (CLI)

Syntax:

```
show interfaces transceiver  [port-list] [detail]
```

Displays information about the transceivers. If a port is specified, displays information for the transceiver in that port.

`detail` Displays detailed transceiver information.

MIB support

The hpicfTransceiver MIB is available for displaying transceiver information.

Viewing transceiver information

The transceiver information displayed depends on the `show` command executed.

Example 65 Example of output for a specified transceiver

The output for `show interfaces transceiver [`*`port-list`*`]` is shown below. You can specify multiple ports, separated by commas, and the information for each transceiver will display.

```
HP Switch(config)# show interfaces transceiver 21

Transceiver Technical information:

                        Product      Serial             Part
 Port    Type           Number       Number             Number
 ------- ----------- ------------ ------------------ ----------
 21      1000SX      J4858C       MY050VM9WB         1990-3657
```

Example 66 Example of output when no transceiver is present in specified interface

If there is no transceiver in the port specified in the command, the output displays as shown below.

```
HP Switch(config)# show interfaces transceiver 22

 No Transceiver found on interface 22
```

Example 67 Example of output when no ports are specified

When no ports are specified, information for all transceivers found is displayed.

```
HP Switch(config)# show interfaces transceiver

 Transceiver Technical information:

                         Product      Serial             Part
  Port    Type           Number       Number             Number
  ------- ----------- ------------ ------------------ ----------
  21      1000SX      J4858C       MY050VM9WB         1990-3657
  22      1000SX      J4858B       P834DIP2
```

Example 68 Example of output when "all" is specified

You can specify all for `port-list` as shown below.

```
HP Switch(config)# show interfaces transceiver all

 No Transceiver found on interface 1

 No Transceiver found on interface 2
.
.
.
 No Transceiver found on interface 24

 Transceiver Technical information:

                         Product      Serial             Part
  Port    Type           Number       Number             Number
  ------- ----------- ------------ ------------------ ----------
  21      1000SX      J4858C       MY050VM9WB         1990-3657
  22      1000SX      J4858B       P834DIP2
```

Information displayed with the detail parameter

When the `show interfaces transceiver [port-list] detail` command is executed, the following information displays.

Table 35 General transceiver information

Parameter	Description
Interface Index	The switch interface number
Transceiver-type	Pluggable transceiver type
Transceiver model	Pluggable transceiver model
Connector-type	Type of connector of the transceiver
Wavelength	For an optical transceiver: the central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, the values will be separated by a comma.
Transfer Distance	Link-length supported by the transceiver in meters. The corresponding transfer medium is shown in brackets following the transfer distance value, for example, 50um multimode fiber. If the transceiver supports multiple transfer media, the values are separated by a comma.
Diagnostic Support	Shows whether the transceiver supports diagnostics: None Supported DOM Supported VCT Supported
Serial Number	Serial number of the transceiver

The information in Table 36 (page 410), Table 37 (page 410), and Table 38 (page 411) is only displayed when the transceiver supports DOM.

Table 36 DOM information

Parameter	Description
Temperature	Transceiver temperature (in degrees Centigrade)
Voltage	Supply voltage in transceiver (Volts)
Bias	Laser bias current (mA)
RX power	Rx power (mW and dBm))
TX power	Tx power (mW and dBm)

The alarm information for GBIC/SFP transceivers is shown in Table 37 (page 410).

Table 37 Alarm and error information (GBIC/SFP transceivers only)

Alarm	Description
RX loss of signal	Incoming (RX) signal is lost
RX power high	Incoming (RX) power level is high
RX power low	Incoming (RX) power level is low
TX fault	Transmit (TX) fault
TX bias high	TX bias current is high
TX bias low	TX bias current is low
TX power high	TX power is high
TX power low	TX power is low
Temp high	Temperature is high
Temp low	Temperature is low

Table 37 Alarm and error information (GBIC/SFP transceivers only) *(continued)*

Alarm	Description
Voltage High	Voltage is high
Voltage Low	Voltage is low

The alarm information for XENPAK transceivers is shown in Table 38 (page 411).

Table 38 Alarm and error information (XENPAK transceivers)

Alarm	Description
WIS local fault	WAN Interface Sublayer local fault
Receive optical power fault	Receive optical power fault
PMA/PMD receiver local fault	Physical Medium Attachment/Physical Medium Dependent receiver local fault
PCS receiver local fault	Physical Coding Sublayer receiver local fault
PHY XS receive local fault	PHY Extended Sublayer receive local fault
RX power high	RX power is high
RX power low	RX power is low
Laser bias current fault	Laser bias current fault
Laser temperature fault	Laser temperature fault
Laser output power fault	Laser output power fault
TX fault	TX fault
PMA/PMD transmitter local fault	PMA/PMD transmitter local fault
PCS Transmit local fault	PCS transmit local fault
PHY XS transmit local fault	PHY SX transmit local fault
TX bias high	TX bias current is high
TX bias low	TX bias current is low
TX power high	TX power is high
TX power low	TX power is low
Temp high	Temperature is high
Temp low	Temperature is low

Example 69 Example of detailed information for a 1000SX Mini-GBIC transceiver

An example of the output for the show interfaces transceiver [port-list] detail for a 1000SX transceiver is shown below.

```
HP Switch(config)# show interfaces transceiver 21 detail

 Transceiver in 21
  Interface index    : 21
  Type               : 1000SX
  Model              : J4858C
  Connector type     : LC
  Wavelength         : 850nm
  Transfer distance  : 300m (50um), 150m (62.5um),
  Diagnostic support : DOM
  Serial number      : MY050VM9WB

 Status
  Temperature : 50.111C
  Voltage     : 3.1234V
  TX Bias     : 6mA
  TX Power    : 0.2650mW, -5.768dBm
  RX Power    : 0.3892mW, -4.098dBm

 Time stamp   :  Mon Mar 7 14:22:13 2011
```

Example 70 Example of detailed information for a 10GbE-LR transceiver

An example of the output for a 10GbE-LR transceiver is shown below.

```
HP Switch(config)# show interfaces transceiver 23 detail

 Transceiver in 23
  Interface Index   : 24
  Type              : 10GbE-LR
  Model             : J8437A
  Connector type    : SC
  Wavelength        : Channel #0: 1310nm, #1:0nm, #2:0nm, #3:0nm
  Transfer distance : 10000m (SM)
  Diagnostic support: DOM
  Serial number     : ED456SS987

 Status
  Temperature : 32.754C
  TX Bias     : 42.700mA
  TX Power    : 0.5192mW, -2.847dBm
  RX Power    : 0.0040mW, -23.979dBm

 Recent Alarms:

  Rx power low alarm
  Rx power low warning

 Recent errors:
  Receive optical power fault
  PMA/PMD receiver local fault
  PMA/PMD transmitter local fault
  PCS receive local fault
  PHY XS transmit local fault

 Time stamp : Mon Mar 7 16:26:06 2011
```

Testing the Cable

Enter the `test cable-diagnostics` command in any context to begin cable diagnostics for the transceiver. The diagnostic attempts to identify cable faults. The tests may take a few seconds to complete for each interface. There is the potential of link loss during the diagnostic.

Syntax:

`test cable-diagnostics` [port-list]

Invokes cable diagnostics and displays the results.

Example 71 Example of output from test cable-diagnostics command

```
HP Switch # test cable-diagnostics a23-a24

 The ‘test cable-diagnostics’ command will cause a loss of link and will take a few seconds per

 interface to complete.

 Continue (Y/N)? y


MDI  Cable     Distance  Pair  Pair      MDI
 Port  Pair  Status     to Fault  Skew  Polarity  Mode
 ----- ----- ---------- --------- ----- --------- ------
 A23   1-2   OK         0 m       6 ns  Normal    MDIX
       3-6   OK         0 m       0 ns  Normal
       4-5   OK         0 m       6 ns  Normal    MDIX
       7-8   OK         0 m       6 ns  Normal
 A24   1-2   Short      2 m
       3-6   Impedance  3 m
       4-5   Impedance  3 m
       7-8   Open       1 m
```

Example 72 Example of copper cable diagnostic test results

```
HP Switch# show interfaces transceiver a23 detail

 Transceiver in A23
  Interface Index   : 23
  Type              : 1000T-sfp
  Model             : J8177C
  Connector Type    : RJ45
  Wavelength        : n/a
  Transfer Distance : 100m (copper),
  Diagnostic Support : VCT
  Serial Number     : US051HF099

  Link Status       : Up
  Speed             : 1000
  Duplex            : Full

       MDI   Cable      Distance  Pair  Pair      MDI
 Port  Pair  Status     to Fault  Skew  Polarity  Mode
 ----- ----- ---------- --------- ----- --------- -----
 A23   1-2   OK         0 m       6 ns  Normal    MDIX
       3-6   OK         0 m       0 ns  Normal
       4-5   OK         0 m       6 ns  Normal    MDIX
       7-8   OK         0 m       6 ns  Normal

   Test Last Run   : Fri Apr 22 20:33:23 2011
```

Table 39 General transceiver information

Parameter	Description
Interface Index	The switch interface number
Transceiver-type	Pluggable transceiver type
Transceiver model	Pluggable transceiver model

Table 39 General transceiver information *(continued)*

Parameter	Description
Connector-type	Type of connector of the transceiver
Wavelength	For an optical transceiver: the central wavelength of the laser sent, in nm. If the transceiver supports multiple wavelengths, the values will be separated by a comma. An electrical transceiver value is displayed as N/A.
Transfer Distance	Link-length supported by the transceiver in meters. The corresponding transfer medium is shown in brackets following the transfer distance value, for example, 50um multimode fiber. If the transceiver supports multiple transfer media, the values are separated by a comma.
Diagnostic Support	Shows whether the transceiver supports diagnostics: None Supported DOM Supported VCT Supported
Serial Number	Serial number of the transceiver
Link Status	Link up or down
Speed	Speed of transceiver in Mbps
Duplex	Type of duplexing
Cable Status	Values are OK, Open, Short, or Impedance
Distance to Fault	The distance in meters to a cable fault (accuracy is +/- 2 meters); displays 0 (zero) if there is no fault
Pair Skew	Difference in propagation between the fastest and slowest wire pairs
Pair Polarity	Signals on a wire pair are polarized, with one wire carrying the positive signal and one carrying the negative signal.
MDI Mode	The MDI crossover status of the two wire pairs (1&2, 3&6, 4&5, 7&8), will be either MDI or MDIX

Viewing transceiver information for copper transceivers with VCT support

This feature provides the ability to view diagnostic monitoring information for copper transceivers with Virtual Cable Test (VCT) support. The cable quality of the copper cables connected between transceivers can be ascertained using the transceiver cable diagnostics. Results of the diagnostics are displayed with the appropriate CLI show commands and with SNMP using the hpicfTransceiver MIB.

The J8177C 1000Base-T Mini-GBIC is supported.

Using the Event Log for troubleshooting switch problems

The Event Log records operating events in single- or double-line entries and serves as a tool to isolate and troubleshoot problems.

Starting in software release K.13.*xx*, the maximum number of entries supported in the Event Log is increased from 1000 to 2000. Entries are listed in chronological order, from the oldest to the most recent.

Once the log has received 2000 entries, it discards the oldest message each time a new message is received. The Event Log window contains 14 log-entry lines. You can scroll through it to view any part of the log.

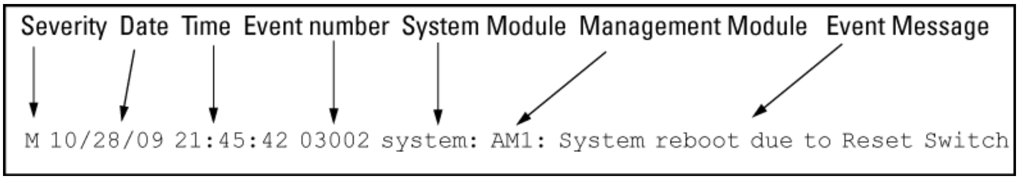
NOTE: The Event Log is *erased* if power to the switch is interruptedor if you enter the `boot system` command. The contents of the Event Log are *not* erased if you:

- Reboot the switch by choosing the `Reboot Switch` option from the menu interface.
- Enter the `reload` command from the CLI.

Event Log entries

As shown in Figure 222 (page 415), each Event Log entry is composed of six or seven fields, depending on whether numbering is turned on or not:

Figure 222 Format of an event log entry



```
M 10/28/09 21:45:42 03002 system: AM1: System reboot due to Reset Switch
```

Item	Description
Severity	One of the followingcodes (from highest to lowest severity): **M**—(major) indicates that a fatal switch error has occurred. **E**—(error) indicates that an error condition occurred on the switch. **W**—(warning) indicates that a switch service has behaved unexpectedly. **I**—(information) provides information on normal switch operation. **D**—(debug) is reserved for HP internal diagnostic information.
Date	Thedate in the format *mm/dd/yy* when an entry is recorded in the log.
Time	The time in the format *hh:mm:ss* when an entry is recorded in the log.
Event number	The number assigned to an event. You can turn event numbering on and off with the `[no] log-number` command.
System module	The internal module (such as "ports:" for port manager) that generated a log entry.If VLANs are configured, a VLAN name also appears for an event that is specific to an individual VLAN. Table C-2 (page 416) lists the different system modules with a description of each one.
Management module	(8200zl switches) is either the active management module represented by AM1 or AM2, or the standby management module, represented by SM1 or SM2.
Event message	A brief description of the operating event.

Table 40 Event Log system modules

System module	Description	Documented in HP Switch hardware/software guide
802.1x	802.1X authentication: Provides access control on a per-client or per-port basis: • Client-level security that allows LAN access to 802.1X clients (up to 32 per port) with valid user credentials • Port-level security that allows LAN access only on ports on which a single 802.1X-capable client (supplicant) has entered valid RADIUS user credentials	*Access Security Guide*
acl	ACLs: Filter layer-3 IP traffic to or from a host to block unwanted IP traffic and block or limit other protocol traffic such as TCP, UDP, IGMP, and ICMP. ACEs specify the filter criteria and an action (permit or deny) to take on a packet if it meets the criteria.	*Advanced Traffic Management Guide*
addrmgr	Address Table Manager: Manages MAC addresses that the switch has learned and are stored in the switch's address table.	*Management and Configuration Guide*
arp-protect	Dynamic ARP Protection: Protects the network from ARP cache poisoning. Only valid ARP requests and responses are relayed or used to update the local ARP cache. ARP packets with invalid IP-to-MAC address bindings advertised in the source protocol address and source physical address fields are discarded.	*Access Security Guide*
auth	Authorization: A connected client must receive authorization through web, AMC, RADIUS-based, TACACS+-based, or 802.1X authentication before it can send traffic to the switch.	*Access Security Guide*
cdp	Cisco Discovery Protocol: Supports reading CDP packets received from neighbor devices, enabling a switch to learn about adjacent CDP devices. HP does not support the transmission of CDP packets to neighbor devices.	*Management and Configuration Guide*
chassis	Hardware operation, including modules and ports, power supply, fans, transceivers, CPU interrupt errors, switch temperature, and so on. Chassis messages include events on POE operation.	*Installation Guides Management and Configuration Guide*
connfilt	Connection-rate filtering: Used on the network edge to protect the network from attack by worm-like malicious code by detecting hosts that are generating IP traffic that exhibits this behavior and (optionally) either	*Access Security Guide*

Table 40 Event Log system modules *(continued)*

System module	Description	Documented in HP Switch hardware/software guide
	throttling or dropping all IP traffic from the offending hosts. Connection-rate filtering messages include events on virus throttling. Virus throttling uses connection-rate filtering to stop the propagation of malicious agents.	
console	Console interface used to monitor switch and port status, reconfigure the switch, and read the event log through an in-band Telnet or out-of-band connection.	*Installation and Getting Started Guide*
cos	Class of Service (CoS): Provides priority handling of packets traversing the switch, based on the IEEE 802.1p priority carried by each packet. CoS messages also include QoS events. The QoS feature classifies and prioritizes traffic throughout a network, establishing an end-to-end traffic priority policy to manage available bandwidth and improve throughput of important data.	*Advanced Traffic Management Guide*
dca	Dynamic Configuration Arbiter (DCA) determines the client-specific parameters that are assigned in an authentication session.	*Access Security Guide*
dhcp	Dynamic Host Configuration Protocol (DHCP) server configuration: Switch is automatically configured from a DHCP (Bootp) server, including IP address, subnet mask, default gateway, Timep Server address, and TFTP server address.	*Management and Configuration Guide*
dhcp v6c	DHCP for IPv6 prefix assignment	*IPv6 Configuration Guide*
dhcpr	DHCP relay: Forwards client-originated DHCP packets to a DHCP network server.	*Advanced Traffic Management Guide*
download	Download operation for copying a software version or files to the switch.	*Management and Configuration Guide*
dhcp-snoop	DHCP snooping: Protects your network from common DHCP attacks, such as address spoofing and repeated address requests.	*Access Security Guide*
dma	Direct Access Memory (DMA): Transmits and receives packets between the CPU and the switch. Not used for logging messages in software release K.13.*xx*.	—
fault	Fault Detection facility, including response policy and the sensitivity level at which a network problem should generate an alert.	*Management and Configuration Guide*

Table 40 Event Log system modules *(continued)*

System module	Description	Documented in HP Switch hardware/software guide
ffi	Find, Fix, and Inform: Event or alert log messages indicating a possible topology loop that causes excessive network activity and results in the network running slow. FFI messages include events on transceiver connections with other network devices.	*Installation and Getting Started Guide* *Management and Configuration Guide*
garp	Generic Attribute Registration Protocol (GARP), defined in the IEEE 802.1D-1998 standard.	*Advanced Traffic Management Guide*
gvrp	GARP VLAN Registration Protocol (GVRP): Manages dynamic 802.1Q VLAN operations, in which the switch creates temporary VLAN membership on a port to provide a link to another port in the same VLAN on another device.	*Advanced Traffic Management Guide*
hpesp	Management module that maintains communication between switch ports.	*Installation and Getting Started Guide*
idm	Identity-driven Management: Optional management application used to monitor and control access to switch.	*Advanced Traffic Management Guide*
igmp	Internet Group Management Protocol: Reduces unnecessary bandwidth usage for multicast traffic transmitted from multimedia applications on a per-port basis.	*Multicast and Routing Guide*
inst-mon	Instrumentation Monitor: Identifies attacks on the switch by generating alerts for detected anomalies.	*Access Security Guide*
ip	IP addressing: Configures the switch with an IP address and subnet mask to communicate on the network and support remote management access; configures multiple IP addresses on a VLAN; enables IP routing on the switch.	*Management and Configuration Guide* *Multicast and Routing Guide*
ipaddrmgr	IP Address Manager: Programs IP routing information in switch hardware.	*Multicast and Routing Guide*
iplock	IP Lockdown: Prevents IP source address spoofing on a per-port and per-VLAN basis by forwarding only the IP packets in VLAN traffic that contain a known source IP address and MAC address binding for the port.	*Access Security Guide*
ipx	Novell Netware protocol filtering: On the basis of protocol type, the switch can forward or drop traffic to a specific set of destination ports on the switch.	*Access Security Guide*

Table 40 Event Log system modules *(continued)*

System module	Description	Documented in HP Switch hardware/software guide
licensing	HP Switch premium licensing: Provides access to expanded features on certain HP switches.	*Premium License Installation Guide*
kms	Key Management System: Configures and maintains security information (keys) for all routing protocols, including a timing mechanism for activating and deactivating an individual protocol.	*Access Security Guide*
lacp	LACP trunks: The switch can either automatically establish an 802.3ad-compliant trunk group or provide a manually configured, static LACP trunk.	*Management and Configuration Guide*
ldbal	Load balancing in LACP port trunks or 802.1s Multiple Spanning Tree protocol (MSTP) that uses VLANs in a network to improve network resource utilization and maintain a loop-free environment. Load-balancing messages also include switch meshing events. The switch meshing feature provides redundant links, improved bandwidth use, and support for different port types and speeds.	*Management and Configuration Guide* *Advanced Traffic Management Guide*
lldp	Link-Layer Discovery Protocol: Supports transmitting LLDP packets to neighbor devices and reading LLDP packets received from neighbor devices, enabling a switch to advertise itself to adjacent devices and to learn about adjacent LLDP devices.	*Management and Configuration Guide*
loop_protect	Loop protection: Detects the formation of loops when an unmanaged device on the network drops spanning tree packets and provides protection by transmitting loop protocol packets out ports on which loop protection has been enabled.	*Advanced Traffic Management Guide*
macauth	Web and MAC authentication: Port-based security employed on the network edge to protect private networks and the switch itself from unauthorized access using one of the following interfaces: • Web page login to authenticate users for access to the network • RADIUS server that uses a device's MAC address for authentication	*Access Security Guide*
maclock	MAC lockdown and MAC lockout • MAC lockdown prevents station movement and MAC address "hijacking" by requiring a MAC address to be used only on an	*Access Security Guide*

Table 40 Event Log system modules *(continued)*

System module	Description	Documented in HP Switch hardware/software guide
	assigned port on the switch. MAC Lockdown also restricts the client device to a specific VLAN. - MAC lockout blocks a specific MAC address so that the switch drops all traffic to or from the specified address.	
mgr	HP PCM and PCM+: Windows-based network management solutions for managing and monitoring performance of HP switches. PCM messages also include events for configuration operations.	*Management and Configuration Guide*
mld	Multicast Listener Discovery (MLD): IPv6 protocol used by a router to discover the presence of multicast listeners. MLD can also optimize IPv6 multicast traffic flow with the snooping feature.	*Multicast and Routing Guide*
mtm	Multicast Traffic Manager (MTM): Controls and coordinates L3 multicast traffic for upper layer protocols.	*Multicast and Routing Guide*
netinet	Network Internet: Monitors the creation of a route or an Address Resolution Protocol (ARP) entry and sends a log message in case of failure.	*Advanced Traffic Management Guide*
ospf	Open Short Path First (OSPF): A routing protocol that uses link-state advertisements (LSA) to update neighboring routers regarding its interfaces and information on those interfaces. Each routing switch maintains an identical database that describes its area topology to help a router determine the shortest path between it and any neighboring router.	*Multicast and Routing Guide*
pagp	Ports Aggregation Protocol (PAgP): Obsolete. Replaced by LACP (802.3ad). Not used for logging messages in software release K.13.*xx*.	—
pim	Protocol-independent multicast (PIM) routing: Enables IP multicast traffic to be transmitted for multimedia applications throughout a network without being blocked at routed interface (VLAN) boundaries.	*Multicast and Routing Guide*
ports	Port status and port configuration features, including mode (speed and duplex), flow control, broadcast limit, jumbo packets, and security settings. Port messages include events on POE operation and transceiver connections with other network devices.	*Installation and Getting Started Guide* *Management and Configuration Guide* *Access Security Guide*

Table 40 Event Log system modules *(continued)*

System module	Description	Documented in HP Switch hardware/software guide
QinQ	IEEE 802.1ad specification, known as QinQ (provider bridging), provides a second tier of VLANs in a bridged network. QinQ supports the forwarding of traffic from multiple customers over a provider network using service VLANs (S-VLANs).	*Advanced Traffic Management Guide*
radius	RADIUS (Remote Authentication Dial-In User Service) authentication and accounting: A network server is used to authenticate user-connection requests on the switch and collect accounting information to track network resource usage.	*Access Security Guide*
ratelim	Rate-limiting: Enables a port to limit the amount of bandwidth a user or device may utilize for inbound traffic on the switch.	*Management and Configuration Guide*
sflow	Flow sampling: sFlow is an industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.	*Management and Configuration Guide*
snmp	Simple Network Management Protocol: Allows you to manage the switch from a network management station, including support for security features, event reporting, flow sampling, and standard MIBs.	*Management and Configuration Guide*
sntp	Simple Network Time Protocol: Synchronizes and ensures a uniform time among interoperating devices.	*Management and Configuration Guide*
ssh	Secure Shell version 2 (SSHv2): Provides remote access to management functions on a switch via encrypted paths between the switch and management station clients capable of SSH operation. SSH messages also include events from the Secure File Transfer Protocol (SFTP) feature. SFTP provides a secure alternative to TFTP for transferring sensitive information, such as switch configuration files, to and from the switch in an SSH session.	*Access Security Guide*
ssl	Secure Socket Layer Version 3 (SSLv3), including Transport Layer Security (TLSv1) support: Provides remote web access to a switch via encrypted paths between the switch and management station clients capable of SSL/TLS operation.	*Access Security Guide*
stack	Stack management: Uses a single IP address and standard network cabling to manage a group (up to 16) of	*Advanced Traffic Management Guide*

Table 40 Event Log system modules *(continued)*

System module	Description	Documented in HP Switch hardware/software guide
	switches in the same IP subnet (broadcast domain), resulting in a reduced number of IP addresses and simplified management of small workgroups for scaling your network to handle increased bandwidth demand.	
stp	Multiple-instance spanning tree protocol/MSTP (802.1s): Ensures that only one active path exists between any two nodes in a group of VLANs in the network. MSTP operation is designed to avoid loops and broadcast storms of duplicate messages that can bring down the network.	*Advanced Traffic Management Guide*
system	Switch management, including system configuration, switch bootup, activation of boot ROM image, memory buffers, traffic and security filters. System messages also include events from management interfaces (menu, CLI, and HP PCM+) used to reconfigure the switch and monitor switch status and performance.	*Management and Configuration Guide* *Access Security Guide*
tacacs	TACACS+ authentication: A central server is used to control access to the switches (and other TACACS-aware devices) in the network through a switch's console port (local access) or Telnet (remote access).	*Access Security Guide*
tcp	Transmission Control Protocol: A transport protocol that runs on IP and is used to set up connections.	*Advanced Traffic Management Guide*
telnet	Session established on the switch from a remote device through the Telnet virtual terminal protocol.	*Management and Configuration Guide*
tftp	Trivial File Transfer Protocol: Supports the download of files to the switch from a TFTP network server.	*Management and Configuration Guide*
timep	Time Protocol: Synchronizes and ensures a uniform time among interoperating devices.	*Management and Configuration Guide*
udld	Uni-directional Link Detection: Monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices.	*Access Security Guide*
udpf	UDP broadcast forwarding: Supports the forwarding of client requests sent as limited IP broadcasts addressed to a UDP application port on a network server.	*Multicast and Routing Guide*

Table 40 Event Log system modules *(continued)*

System module	Description	Documented in HP Switch hardware/software guide
update	Updates (TFTP or serial) to HP switch software and updates to running-config and start-up config files	*Management and Configuration Guide*
usb	Auxiliary port that allows you to connect external devices to the switch.	*Installation and Getting Started Guide*
vlan	Static 802.1Q VLAN operations, including port-and protocol-based configurations that group users by logical function instead of physical location • A port-based VLAN creates a layer-2 broadcast domain comprising member ports that bridge IPv4 traffic among themselves. • A protocol-based VLAN creates a layer-3 broadcast domain for traffic of a particular routing protocol, and comprises member ports that bridge traffic of the specified protocol type among themselves. VLAN messages include events from management interfaces (menu, CLI, and HP PCM+) used to reconfigure the switch and monitor switch status and performance.	*Advanced Traffic Management Guide*
vrrp	Virtual Router Redundancy Protocol: Provides dynamic failover support as backup for gateway IP addresses (first-hop routers) so that if a VR's master router becomes unavailable, the traffic it supports will be transferred to a backup router without major delays or operator intervention, eliminating single-point-of-failure problems.	*Advanced Traffic Management Guide*
xmodem	Xmodem: Binary transfer feature that supports the download of software files from a PC or UNIX workstation.	*Management and Configuration Guide*
xrrp	Extended Router Redundancy Protocol: Routing protocol not used for logging messages in software release K.13.*xx*.	—

Displaying and navigating in the Event Log

Displaying the Event Log

Using the CLI

Syntax:

```
show logging [-a, -b, -r, -s, -t, -m, -p, -w, -i, -d]
[option-str]
```

By default, the `show logging` command displays the log messages recorded since the last reboot in chronological order:

`-a`	Displays all recorded log messages, including those before the last reboot.
`-b`	Displays log events as the time since the last reboot instead of in a date/time format.
`-r`	Displays all recorded log messages, with themost recent entries listed first (reverse order).
`-s`	Displays the active management module (AM) and standby management module (SM) log events.
`-t`	Displays the log events with a granularity of 10 milliseconds.
`-m`	Displays only major log events.
`-p`	Displays only performance log events.
`-w`	Displays only warning log events.
`-i`	Displays only informational log events.
`-d`	Displays only debug log events.
`option-str`	Displays all Event Log entries that contain the specified text. Use an *`option-str`* value with `-a` or `-r` to further filter `show logging` command output.

Example

To display all Event Log messages that have "system" in the message text or module name, enter the following command:

```
HP Switch# show logging -a system
```

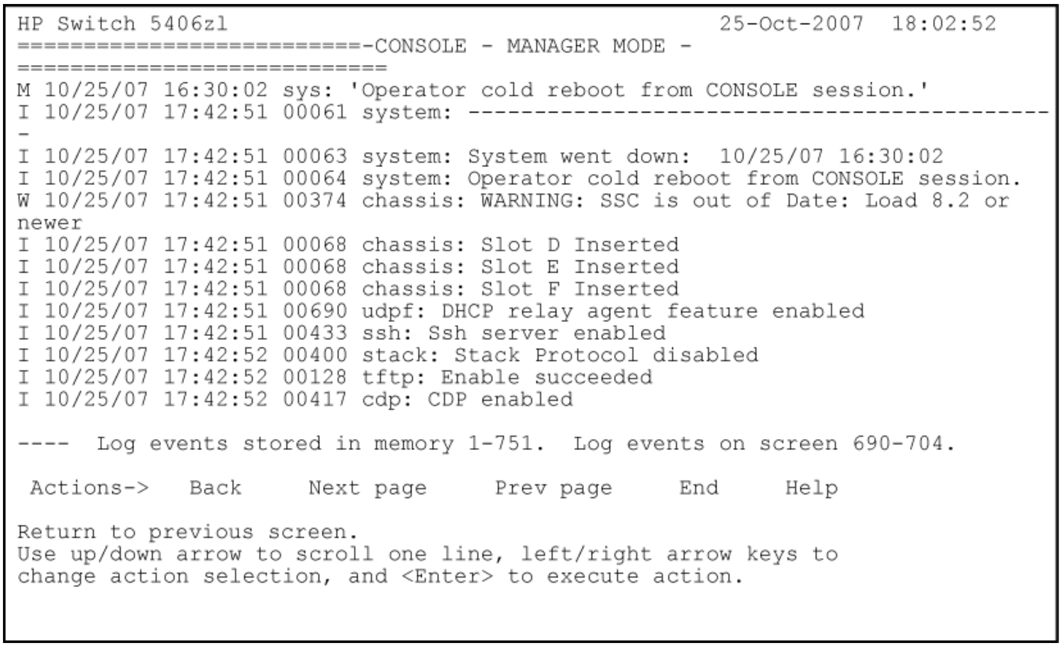
To display all Event Log messages recorded since the last reboot that have the word "system" in the message text or module name, enter:

```
HP Switch# show logging system
```

Using the Menu

To display the Event Log from the Main Menu, select `Event Log`. Figure 223 (page 425) shows a sample event log display.

Figure 223 Example of an event log display



```
HP Switch 5406zl                                    25-Oct-2007  18:02:52
===========================-CONSOLE - MANAGER MODE -
============================
M 10/25/07 16:30:02 sys: 'Operator cold reboot from CONSOLE session.'
I 10/25/07 17:42:51 00061 system: ---------------------------------------
-
I 10/25/07 17:42:51 00063 system: System went down:  10/25/07 16:30:02
I 10/25/07 17:42:51 00064 system: Operator cold reboot from CONSOLE session.
W 10/25/07 17:42:51 00374 chassis: WARNING: SSC is out of Date: Load 8.2 or
newer
I 10/25/07 17:42:51 00068 chassis: Slot D Inserted
I 10/25/07 17:42:51 00068 chassis: Slot E Inserted
I 10/25/07 17:42:51 00068 chassis: Slot F Inserted
I 10/25/07 17:42:51 00690 udpf: DHCP relay agent feature enabled
I 10/25/07 17:42:51 00433 ssh: Ssh server enabled
I 10/25/07 17:42:52 00400 stack: Stack Protocol disabled
I 10/25/07 17:42:52 00128 tftp: Enable succeeded
I 10/25/07 17:42:52 00417 cdp: CDP enabled

----  Log events stored in memory 1-751.  Log events on screen 690-704.

 Actions->   Back     Next page     Prev page     End     Help

Return to previous screen.
Use up/down arrow to scroll one line, left/right arrow keys to
change action selection, and <Enter> to execute action.
```

The *log status line* below the recorded entries states the total number of events stored in the event log and which logged events are currently displayed.

Navigating in the Event Log

Using the Menu

To scroll to other entries in the Event Log, either preceding or following the currently visible portion, press the keys indicated at the bottom of the display (`Back`,`Nextpage`, `Prev page`, or `End`) or the keys described in TableTable 3-3 (page 425).

Table 41 Event Log control keys

Key	Action
[N]	Advances the display by one page (next page).
[P]	Rolls back the display by one page (previous page).
[v]	Advances display by one event (down one line).
[ˆ]	Rolls back display by one event (up one line).
[E]	Advances to the end of the log.
[H]	Displays Help for the Event Log.

Clearing Event Log entries

Syntax:

```
clear logging
```

Removes all entries from the event log display output.

Use the `clear logging` command to hide, but not erase, Event Log entries displayed in `show logging` command output. Only new entries generated after you enter the command will be displayed.

To redisplay all hidden entries, including Event Log entries recorded prior to the last reboot, enter the `show logging -a` command.

Turning event numbering on

Syntax:

```
[ no ] log-numbers
```

Turns event numbering on and off

Using log throttling to reduce duplicate Event Log and SNMP messages

A recurring event can generate a series of duplicate Event Log messages and SNMP traps in a relatively short time. As a result, the Event Log and any configured SNMP trap receivers may be flooded with excessive, exactly identical messages. To help reduce this problem, the switch uses *log throttle periods* to regulate (throttle) duplicate messages for recurring events, and maintains a counter to record how many times it detects duplicates of a particular event since the last system reboot.

When the first instance of a particular event or condition generates a message, the switch initiates a log throttle period that applies to all recurrences of that event. If the logged event recurs during the log throttle period, the switch increments the counter initiated by the first instance of the event, but does not generate a new message.

If the logged event repeats again after the log throttle period expires, the switch generates a duplicate of the first message, increments the counter, and starts a new log throttle period during which any additional instances of the event are counted, but not logged. Thus, for a particular recurring event, the switch displays only one message in the Event Log for each log throttle period in which the event reoccurs. Also, each logged instance of the event message includes counter data showing how many times the event has occurred since the last reboot. The switch manages messages to SNMP trap receivers in the same way.

Log throttle periods

The length of the log throttle period differs according to an event's severity level:

Severity level	Log throttle period
I (Information)	6000 Seconds
W (Warning)	600 Seconds
D (Debug)	60 Seconds
M (Major)	6 Seconds

Example

Suppose that you configure VLAN 100 on the switch to support PIM operation, but do not configure an IP address. If PIM attempts to use VLAN 100, the switch generates the first instance of the following Event Log message and counter.

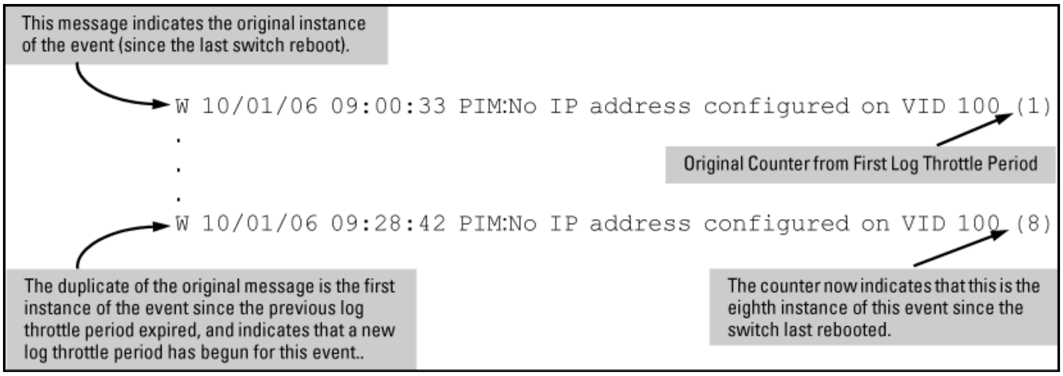
Example 73 The first instance of an event message and counter

The counter (1) indicates that this is the first instance of this event since the switch last rebooted.

```
W 10/01/12 09:00:33 PIM:No IP address configured on VID 100 (1)
```

If PIM operation causes the same event to occur six more times during the initial log throttle period, there are no further entries in the Event Log. However, if the event occurs again after the log throttle period has expired, the switch repeats the message (with an updated counter) and starts a new log throttle period.

Figure 224 Duplicate messages over multiple log throttling periods



This message indicates the original instance of the event (since the last switch reboot).

```
W 10/01/06 09:00:33 PIM:No IP address configured on VID 100 (1)
.
.
.
W 10/01/06 09:28:42 PIM:No IP address configured on VID 100 (8)
```

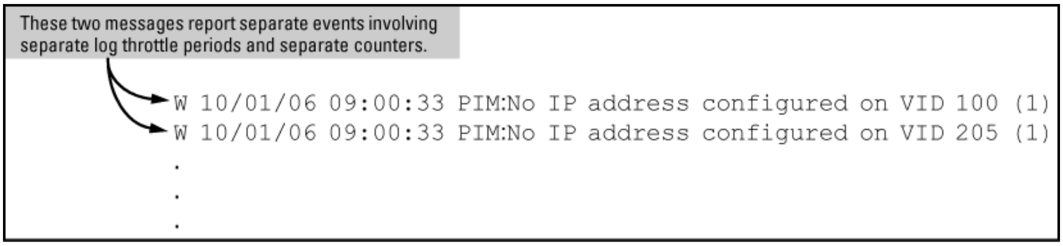
Original Counter from First Log Throttle Period

The duplicate of the original message is the first instance of the event since the previous log throttle period expired, and indicates that a new log throttle period has begun for this event..

The counter now indicates that this is the eighth instance of this event since the switch last rebooted.

Note that if the same type of event occurs under different circumstances, the switch handles these as unrelated events for the purpose of Event Log messages. For example, if PIM operation simultaneously detects that VLANs 100 and 205 are configured without IP addresses, you see log messages similar to the following:

Figure 225 Example of log messages generated by unrelated events of the same type



These two messages report separate events involving separate log throttle periods and separate counters.

```
W 10/01/06 09:00:33 PIM:No IP address configured on VID 100 (1)
W 10/01/06 09:00:33 PIM:No IP address configured on VID 205 (1)
.
.
.
```

Example of event counter operation

Suppose the switch detects the following after a reboot:

- Three duplicate instances of the PIM "Send error" during the first log throttle period for this event
- Five more instances of the same Send error during the second log throttle period for this event
- Four instances of the same Send error during the third log throttle period for this event

In this case, the duplicate message appears three times in the Event Log (once for each log throttle period for the event being described), and the duplicate message counter increments as shown in Table 3-4 (page 427). (The same operation applies for messages sent to any configured SNMP trap receivers.)

Table 42 How the duplicate message counter increments

Instances during 1st log throttle period	Instances during 2nd log throttle period	Instances during 3rd log throttle period	Duplicate message counter[1]
3			1
	5		4
		4	9

[1] This value always comprises the first instance of the duplicate message in the current log throttle period plus all previous occurrences of the duplicate message occurring since the switch last rebooted.

Debug/syslog operation

While the Event Log records switch-level progress, status, and warning messages on the switch, the debug/system logging (*syslog*) feature provides a way to record Event Log and debug messages on a remote device. For example, you can send messages about routing misconfigurations and other network protocol details to an external device, and later use them to debug network-level problems.

Debug/syslog messaging

The debug/syslog feature allows you to specify the types of Event Log and debug messages that you want to send to an external device. You can perform the following operations:

- Use the `debug` commandto configure messaging reports for the following event types:
  - ACL "deny" matches
  - Dynamic ARP protection events
  - DHCP snooping events
  - DIPLD events
  - Events recorded in the switch's Event Log
  - IPv4 routing events
  - LACP events
  - LLDP events
  - OSPF events
  - PBR class events
  - SNMP events
  - SSH events
  - VRRP events
  - Wireless services events
- Use the `logging` commandto select a subset of Event Log messages to send to an external device for debugging purposes according to:
  - Severity level
  - System module

Debug/syslog destination devices

To use debug/syslog messaging, you must configure an external device as the logging destination by using the `logging` and `debug destination` commands. For more information, see "Enabling or disabling syslog messaging" (page 440) and "Configuring a syslog server" (page 441).

A debug/syslog destination device can be a syslog server and/or a console session. You can configure debug and logging messages to be sent to:

- Up to six syslog servers
- A CLI session through a direct RS-232 console connection, or a Telnet or SSH session

Debug/syslog configuration commands

Event notification logging	—	Automatically sends switch-level event messages to the switch's Event Log. Debug and syslog do not affect this operation, but add the capability of directing Event Log messaging to an external device.
`logging` Command	*`syslog-ip-addr`*	Enables syslog messaging to be sent to the specified IP address. IPv4 and IPv6 are supported.

	`facility`	(Optional) The `logging facility` command specifies the destination (facility) subsystem used on a syslog server for debug reports.
	`priority-desc`	A text string associated with the values of facility, severity, and system-module.
	`neighbor-adjacency` [detail]	Enables or disables OSPFv3 (IPv6) adjacency logging. Must be executed in OSPFv3 context. The `detail` option displays all the adjacency state transitions and adjacency-related errors.
	`severity`	Sends Event Log messages of equal or greater severity than the specified value to configured debug destinations. (The default setting is to send Event Log messages from all severity levels.)
	`system-module`	Sends Event Log messages from the specified system module to configured debug destinations. The severity filter is also applied to the system-module messages you select. The default setting is to send Event Log messages from all system modules. To restore the default setting, enter the `no logging system-module` *`system-module`* or `logging system-module all-pass` commands.
`debug` Command	`acl`	Sends ACL syslog logging to configured debug destinations. When there is a match with a "deny" statement, directs the resulting message to the configured debug destinations.
	`all`	Sends debug logging to configured debug destinations for all ACL, Event Log, IP-OSPF, and IP-RIP options.
	`cdp`	Displays CDP information.
	`destination`	`logging`: Disables or re-enables syslog logging on one or more syslog servers configured with the `logging` *`syslog-ip-addr`* command. `session`: Assigns or re-assigns destination status to the terminal device that was most recently used to request debug output. `buffer`: Enables syslog logging to send the debug message types specified by the `debug` *`debug-type`* command to a buffer in switch memory. For more information on these options, see "Enabling or disabling syslog messaging" (page 440).
	`event`	Sends standard Event Log messages to configured debug destinations. (The same messages are also sent to the switch's Event Log, regardless of whether you enable this option.)

	ip	fib: Displays IP Forwarding Information Base messages and events. forwarding: Sends IPv4 forwarding messages to the debug destinations. ospf: Sends OSPF event logging to the debug destinations. ospfv3: Enables debug messages for OSPFv3. packet: Sends IPv4 packet messages to the debug destinations. pim [packet [filter source *ip-addr* | vlan *vid*]] : Enables or disables tracing of PIM messages. **Note**: When PIM debugging is enabled, the following message displays: `PIM Debugging can be extremely CPU intensive when run on a device with an existing high CPU load or on a switch with more than 10 PIM-enabled VLANs. In high load situations, the switch may suffer from protocol starvation, high latency, or even reload. When debugging a switch with more than 10 PIM-enabled VLANs, the` **“vlan”** `option in` **“debug ip pim packet”** `should be utilized. Debugging should only be used temporarily while troubleshooting problems. Customers are advised to exercise caution when running this command in a highstress production network.` pbr: Logs a message when a PBR policy is applied, when the action in a class goes active or when it goes inactive. rip: Sends RIP event logging to the debug destinations.
	ipv6	dhcpv6-client: Sends DHCPv6 client debug messages to the configured debug destination. dhcpv6-relay: Sends DHCPv6 relay debug messages to the configured debug destination. forwarding: Sends IPv6 forwarding messages to the debug destination(s) nd: Sends IPv6 debug messages for IPv6 neighbor discovery to the configured debug destinations.
		ospf3[adj | event | flood | lsa-generation | packet | retransmission | spf] : Sends OSPFv3 events to the debug destinations. Must be executed in

		OSPFv3 context. Selecting an option filters the debug messages by that option. `packet`: Sends IPv6 packet messages to the debug destinations.
	`lldp`	Sends LLDP debug messages to the debug destinations.
	`lacp`	`event`: Sends messages related to change events. `packet`: Sends messages when BPDUs are exchanged.
	`security`	Sends security messages to the debug destination.
	`services`	Displays debug messages on the services module.
	`snmp`	Sends snmp messages to the debug destination.
	`vrrp`	Turns on tracing of the incoming and outgoing VRRP packets and sends debug logging to the debug destination.
	`wireless-services`	Sends wireless service module debug messages to the debug destination.

Using the Debug/Syslog feature, you can perform the following operations:

- Configure the switch to send Event Log messages to one or more Syslog servers. In addition, you can configure the messages to be sent to the User log facility (default) or to another log facility on configured Syslog servers.
- Configure the switch to send Event Log messages to the current management- access session (serial-connect CLI, Telnet CLI, or SSH).
- Disable all Syslog debug logging while retaining the Syslog addresses from the switch configuration. This allows you to configure Syslog messaging and then disable and re-enable it as needed.
- Display the current debug configuration. If Syslog logging is currently active, the list f configured Syslog servers is displayed.
- Display the current Syslog server list when Syslog logging is disabled.

Configuring debug/syslog operation

1. To use a syslog server as the destination device for debug messaging, follow these steps:
   a. Enter the `logging` *`syslog-ip-addr`* command at the global configuration level to configure the syslog server IP address and enable syslog logging. Optionally, you may also specify the destination subsystem to be used on the syslog server by entering the `logging facility` command.

      If no other syslog server IP addresses are configured, entering the `logging` command enables both debug messaging to a syslog server and the event debug message type. As a result, the switch automatically sends Event Log messages to the syslog server, regardless of other debug types that may be configured.

   b. Re-enter the `logging` command in step "a (page 431)" to configure additional syslog servers. You can configure up to a total of six servers. (When multiple server IP addresses are configured, the switch sends the debug message types that you configure in step 3 (page 432) to all IP addresses.)
2. To use a CLI session on a destination device for debug messaging:

   a. Set up a serial, Telnet, or SSH connection to access the switch's CLI.
   b. Enter the debug destination session command at the manager level.

3. Enable the types of debug messages to be sent to configured syslog servers, the current session device, or both by entering the debug *debug-type* command and selecting the desired options.

   Repeat this step if necessary to enable multiple debug message types.

   By default, Event Log messages are sent to configured debug destination devices. To block Event Log messages from being sent, enter the no debug event command.

4. If necessary, enable a subset of Event Log messages to be sent to configured syslog servers by specifying a severity level, a system module, or both using the following commands

   ```
   HP Switch(config)# logging severity
   [  debug  |   major  |   error  |   warning  |   info  ]
   ```

   ```
   HP Switch(config)# logging system-module  system-module
   ```

   To display a list of valid values for each command, enter logging severity or logging system-module followed by ? or pressing the Tab key.

   The severity levels in order from the highest to lowest severity are major, error, warning, info, and debug. For a list of valid values for the logging system-module *system-module* command, see Table C-2 (page 416).

5. If you configure system-module, severity-level values, or both to filter Event Log messages, when you finish troubleshooting, you may want to reset these values to their default settings so that the switch sends all Event Log messages to configured debug destinations (syslog servers, CLI session, or both).

   To remove a configured setting and restore the default values that send all Event Log messages, enter one or both of the following commands:

   ```
   HP Switch(config)# no logging severity
   [  debug  |   major  |   error  |   warning  |   info ]
   ```

   ```
   HP Switch(config)# no logging system-module  system-module
   ```

△ **CAUTION:** If you configure a severity-level, system-module, logging destination, or logging facility value and save the settings to the startup configuration (for example, by entering the write memory command), the debug settings are saved after a system reboot (power cycle or reboot) and re-activated on the switch. As a result, after switch startup, one of the following situations may occur:

- Only a partial set of Event Log messages may be sent to configured debug destinations.
- Messages may be sent to a previously configured syslog server used in an earlier debugging session.

Viewing a debug/syslog configuration

Use the show debug command to display the currently configured settings for:

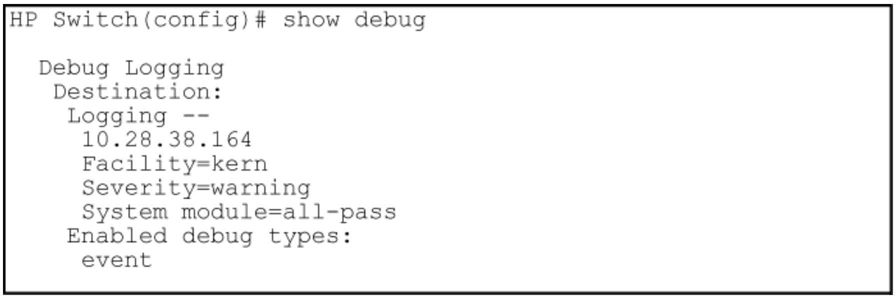
- Debug message types and Event Log message filters (severity level and system module) sent to debug destinations
- Debug destinations (syslog servers or CLI session) and syslog server facility to be used

Syntax:

```
show debug
```

Displays the currently configured debug logging destinations and message types selected for debugging purposes. (If no syslog server address is configured with the `logging` *`syslog-ip-addr`* command, no `show debug` command output is displayed.)

Figure 226 Sample output of `show debug` command

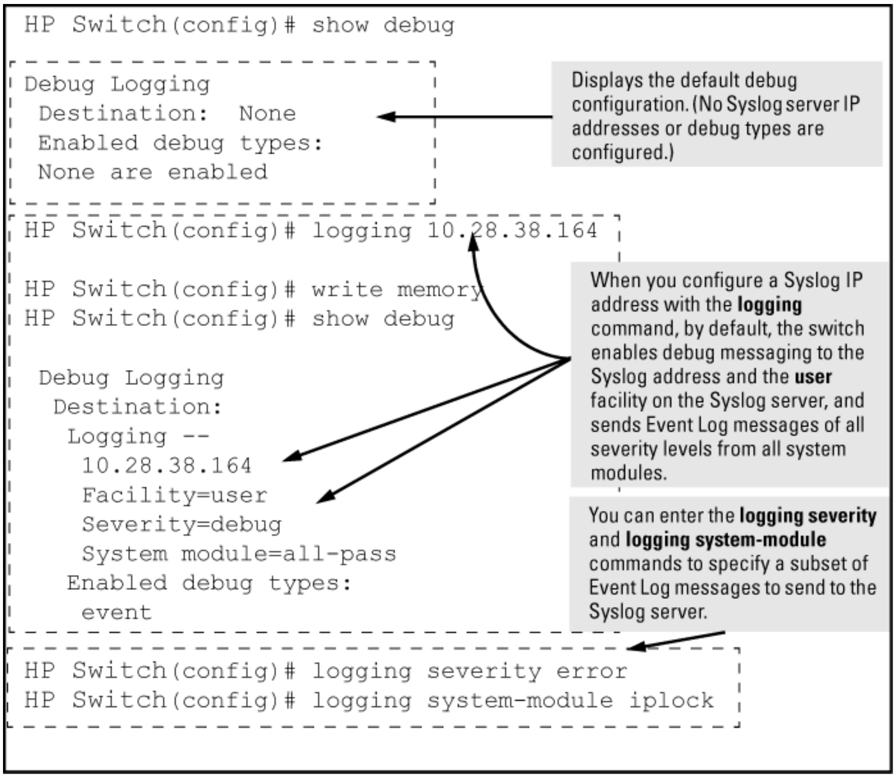


```
HP Switch(config)# show debug

  Debug Logging
   Destination:
    Logging --
     10.28.38.164
     Facility=kern
     Severity=warning
     System module=all-pass
    Enabled debug types:
     event
```

Example

In the following example, no syslog servers are configured on the switch (default setting). When you configure a syslog server, debug logging is enabled to send Event Log messages to the server. To limit the Event Log messages sent to the syslog server, specify a set of messages by entering the `logging severity` and `logging system-module` commands.

Figure 227 Syslog configuration to receive event log messages from specified system module and severity levels



```
 HP Switch(config)# show debug

 Debug Logging
  Destination:  None
  Enabled debug types:
  None are enabled

 HP Switch(config)# logging 10.28.38.164

 HP Switch(config)# write memory
 HP Switch(config)# show debug

  Debug Logging
   Destination:
    Logging --
     10.28.38.164
     Facility=user
     Severity=debug
     System module=all-pass
    Enabled debug types:
     event

 HP Switch(config)# logging severity error
 HP Switch(config)# logging system-module iplock
```

Displays the default debug configuration. (No Syslog server IP addresses or debug types are configured.)

When you configure a Syslog IP address with the **logging** command, by default, the switch enables debug messaging to the Syslog address and the **user** facility on the Syslog server, and sends Event Log messages of all severity levels from all system modules.

You can enter the **logging severity** and **logging system-module** commands to specify a subset of Event Log messages to send to the Syslog server.

As shown at the top of Figure 227 (page 433), if you enter the `show debug` command when no syslog server IP address is configured, the configuration settings for syslog server facility, Event Log severity level, and system module are not displayed. However, after you configure a syslog server address and enable syslog logging, all debug and logging settings are displayed with the `show debug` command.

If you do not want Event Log messages sent to syslog servers, you can block the messages from being sent by entering the `no debug event` command. (There is no effect on the normal logging of messages in the switch's Event Log.)

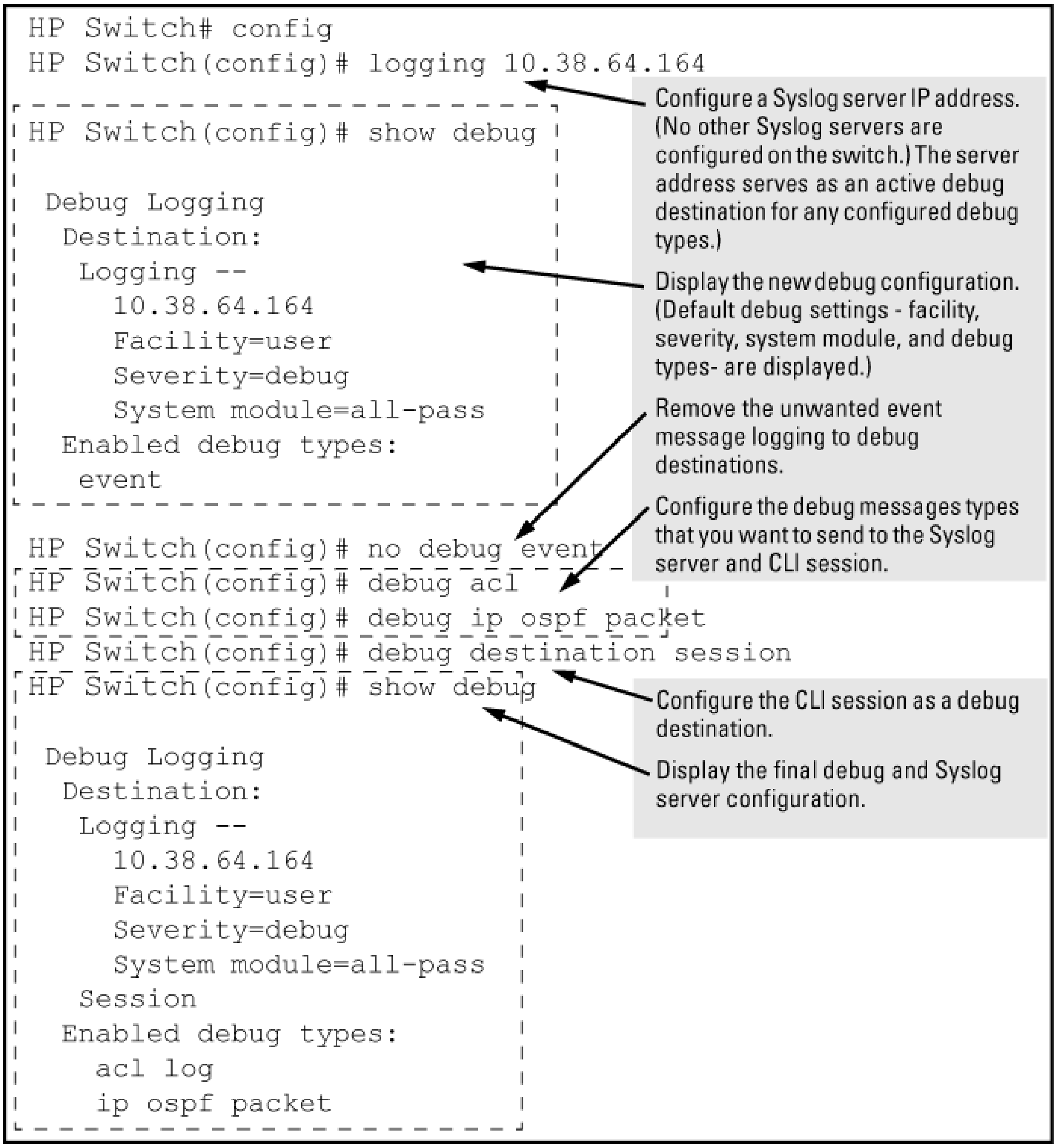
Example

The next example shows how to configure:

- Debug logging of ACL and IP-OSPF packet messages on a syslog server at 18.38.64.164 (with user as the default logging facility).
- Display of these messages in the CLI session of your terminal device's management access to the switch.
- Blocking Event Log messages from being sent from the switch to the syslog server and a CLI session.

To configure syslog operation in these ways with the debug/syslog feature disabled on the switch, enter the commands shown in Figure 228 (page 434).

Figure 228 Debug/syslog configuration for multiple debug types and multiple destinations



```
HP Switch# config
HP Switch(config)# logging 10.38.64.164

HP Switch(config)# show debug

 Debug Logging
  Destination:
   Logging --
     10.38.64.164
     Facility=user
     Severity=debug
     System module=all-pass
  Enabled debug types:
   event

HP Switch(config)# no debug event
HP Switch(config)# debug acl
HP Switch(config)# debug ip ospf packet
HP Switch(config)# debug destination session
HP Switch(config)# show debug

 Debug Logging
  Destination:
   Logging --
     10.38.64.164
     Facility=user
     Severity=debug
     System module=all-pass
   Session
  Enabled debug types:
    acl log
    ip ospf packet
```

Configure a Syslog server IP address. (No other Syslog servers are configured on the switch.) The server address serves as an active debug destination for any configured debug types.)

Display the new debug configuration. (Default debug settings - facility, severity, system module, and debug types- are displayed.)

Remove the unwanted event message logging to debug destinations.

Configure the debug messages types that you want to send to the Syslog server and CLI session.

Configure the CLI session as a debug destination.

Display the final debug and Syslog server configuration.

Debug command

At the manager level, use the `debug` command to perform two main functions:

- Specify the types of event messages to be sent to an external destination.
- Specify the destinations to which selected message types are sent.

By default, no debug destination is enabled and only Event Log messages are enabled to be sent.

NOTE: To configure a syslog server, use the `logging` *`syslog-ip-addr`* command. For more information, see "Configuring a syslog server" (page 441).

Configuring the types of debug messages that the switch can send to configured debug destinations

Syntax:

```
[ no ] debug  debug-type
```

`acl`	When a match occurs on an ACL "deny" ACE (with `log` configured), the switch sends an ACL message to configured debug destinations. For information on ACLs, see the "Access Control Lists (ACLs)" chapter in the latest version of the following guides: IPv4 ACLs: *Access Security Guide* IPv6 ACLs: *IPv6 Configuration Guide* **NOTE:** Beginning with software release K.14.01, ACE matches (hits) for permit and deny entries can be tracked using the `show statistics[ aclv4 | aclv6 ]` command. (Default: Disabled—ACL messages for traffic that matches "deny" entries are not sent.)
`all`	Configures the switch to send all debug message types to configured debug destinations. (Default: Disabled—No debug messages are sent.)
`cdp`	Sends CDP information to configured debug destinations.
`destination`	`logging`—Disables or re-enables syslog logging on one or more syslog servers configured with the `logging` *`syslog-ip-addr`* command. `session`—Assigns or re-assigns destination status to the terminal device that was most recently used to request debug output. `buffer`—Enables syslog logging to send the debug message types specified by the `debug` *`debug-type`* command to a buffer in switch memory. For more information on these options, see "Enabling or disabling syslog messaging" (page 440).
`event`	Configures the switch to send Event Log messages to configured debug destinations. **NOTE:** This value does not affect the reception of event notification messages in the Event Log on the switch.

	Event Log messages are automatically enabled to be sent to debug destinations in these conditions: • If no syslog server address is configured and you enter the `logging` *`syslog-ip-addr`* command to configure a destination address. • If at least one syslog server address is configured in the startup configuration, and the switch is rebooted or reset. Event log messages are the default type of debug message sent to configured debug destinations.
`ip [fib	forwarding	ospf	ospfv3	packet	pim	rip]`	
	Sends IP messages to configured destinations.
`ip [fib [events]]`	For the configured debug destinations: `events`—Sends IP forwarding information base events.
`ip [ospf [adj	event	flood	lsa-generation	packet` *`packet-type`* `	retransmission	spf]]`	
	For the configured debug destinations: `ospf`—Enables the specified IP-OSPF message type. `adj`—Adjacency changes. `event`—OSPF events. `flood`—Information on flood messages. `lsa-generation`—New LSAs added to database. `packet` [*`packet-type`*] — All OSPF packet messages sent and received on the switch, where *`packet-type`* enables only the specified OSPF packet type. Valid values are: `dd`—Database descriptions `hello`—Hello messages `lsa`—Link-state advertisements `lsr`—Link-state requests `lsu`—Link-state updates `retransmission`—Retransmission timer messages. `spf`—Path recalculation messages.
`ip [ospfv3]`	Enables OSPFv3 debug messages.
`ip [pim [packet filter source` *`ip-addr`* `| vlan` *`vid`* `]]`	
	For the configured debug destinations: `packet`— Enables the specified PIM message type `filter`— Enables or disables tracing of PIM messages filtered on VLAN or source group information.

	`source` *`ip-addr`* — Displays packets from a specific source to a specific group. Only a single source/group filter is supported.
	`vlan` *`vlan-id`*— Enables or disables tracing on a specified VLAN for PIM
	NOTE: When PIM debugging is enabled, the following message displays:
	`PIM Debugging can be extremely CPU`
	`intensive when run on a device with`
	` an`
	`existing high CPU load or on a`
	`switch with`
	`more than 10 PIM-enabled VLANs. In`
	`high`
	`load situations, the switch may`
	`suffer`
	`from protocol starvation, high`
	`latency,`
	`or even reload. When debugging a`
	`switch`
	`with more than 10 PIM-enabled VLANs,`
	` the`
	`“vlan”` `option in` **`“debug ip pim`**
	`packet”`
	`should be utilized. Debugging should`
	` only`
	`be used temporarily while`
	`troubleshooting`
	`problems. Customers are advised to`
	`exercise caution when running this`
	`command in a high-stress production`
	`network.`

`ip [ rip [ database | event | trigger ]]`	
	`rip [ database | event | trigger ]` —Enables the specified RIP message type for the configured destination(s). `database`—Displays database changes. `event`—Displays RIP events. `trigger`—Displays trigger messages.
`ipv6 [ dhcpv6-client | dhcpv6-relay | forwarding | nd | ospfv3 | packet ]`	
	NOTE: See the "IPv6 Diagnostic and Troubleshooting" chapter in the *IPv6 Configuration Guide* for your switch for more detailed IPv6 debug options. When no debug options are included, displays debug messages for all IPv6 debug options. `dhcpv6-client [ events | packe ]` —Displays DHCPv6 client event and packet data. `dhcpv6-relay [ events | packet ]` —Displays DHCPv6 relay event and relay packet data.

	`forwarding`— Displays IPv6 Forwarding Information Base messages. `nd`—Displays debug messages for IPv6 neighbor discovery. `ospfv3`—Enables the specified IPv6-OSPF message type. `adj`— Adjacency changes. `event`— OSPFv3 events. `flood`— Information on flood messages. `lsa-generation`— New link state advertisements added to database. `packet` [`packet-type`] —All OSPFv3 packet messages sent and received on the switch, where packet-type enables only the specified OSPFv3 packet type. Valid values are: `dd`— Database descriptions `hello`— Hello messages `lsa`— Link-state advertisements `lsr`— Link-state requests `lsu`— Link-state updates `retransmission`—Retransmission timer messages. `spf`—Path recalculation messages. `packet`—Displays IPv6 packet messages.
`lldp`	Enables all LLDP message types for the configured destinations.
`security`[`arp-protect` | `dhcp-snooping` | `dynamic-ip-lockdown` | `port-access` | `port-security` | `radius-server` | `ssh` | `tacacs-server` | `user-profile-mib`]	
	`arp-protect`— Sends dynamic ARP protection debug messages to configured debug destinations. `dhcp-snooping`—Sends DHCP snooping debug messages to configured debug destinations. `agent`—Displays DHCP snooping agent messages. `event`—Displays DHCP snooping event messages. `packet`—Displays DHCP snooping packet messages. `dynamic-ip-lockdown`—Sends dynamic IP lockdown debug messages to the debug destination. `port-access`—Sends port-access debug messages to the debug destination. `radius-server`—Sends RADIUS debug messages to the debug destination. `ssh`—Sends SSH debug messages at the specified level to the debug destination. The levels

	are fatal, error, info, verbose, debug, debug2, and debug3. `tacacs-server`—Sends TACACS debug messages to the debug destination. `user-profile-mib`—Sends user profile MIB debug messages to the debug destination.
`services` *`slot-id-range`*	
	Displays debug messages on the services module. Enter an alphabetic module ID or range of module IDs for the *`slot-id-range`* parameter.
`snmp  event | pdu | routines`	
	Displays the SNMP debug messages. `event`—Displays SNMP event debug messages. `pdu`—Displays SNMP pdu debug messages. `routines`—Displays SNMP routines debug messages
`vrrp`	Displays VRRP debug messages on the configured destinations.
`wireless-services` *`slot-id-range`*	
	Displays wireless-services debug messages on the wireless services module. Enter an alphabetic module ID or range of IDs for the *`slot-id-range`* parameter.

Filtering debug messages by debug type

Debug message filtering provides the ability to filter debug messages by debug type. Multiple debug filters can be applied to a debug type.

Syntax:

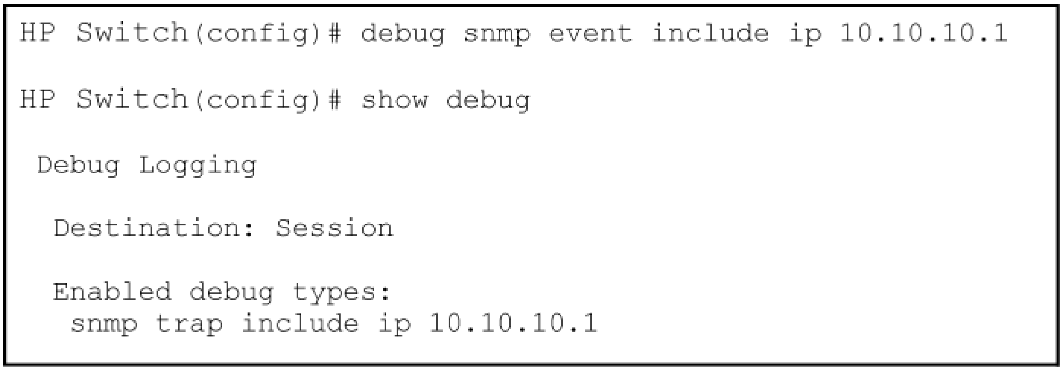
```
[ no ] debug debug type include[ ip ip-addr list | port
port-list  | vlan  vid-list  ]
```

Enables or disables debug message filtering for a debug type. The filter types are:

IPv4 or IPv6 address list Port list VLAN list

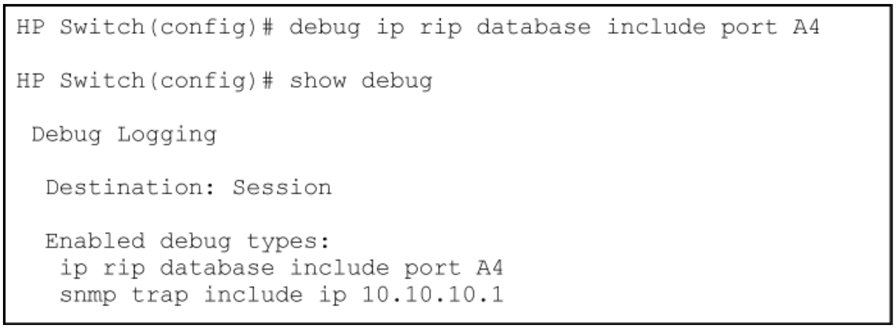
Default: Disabled

Figure 229 Example of setting an SNMP event filter for an IP address



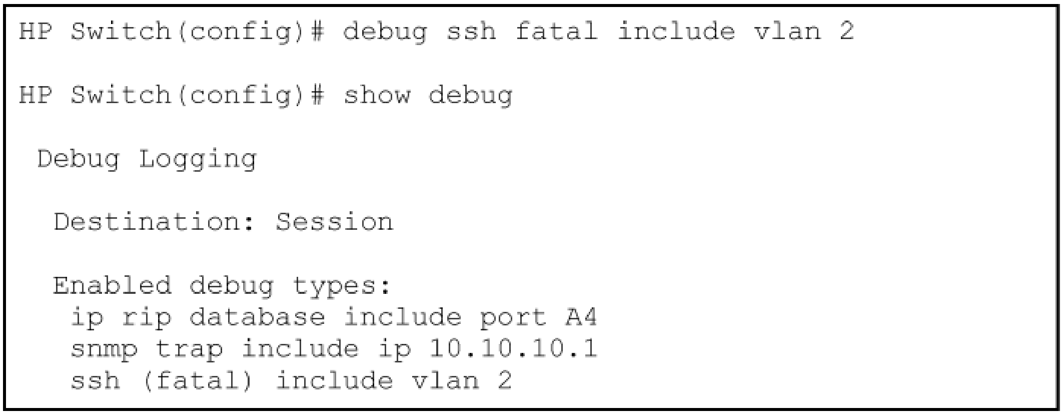
```
HP Switch(config)# debug snmp event include ip 10.10.10.1

HP Switch(config)# show debug

 Debug Logging

  Destination: Session

  Enabled debug types:
   snmp trap include ip 10.10.10.1
```

Figure 230 Example of setting an IP RIP filter for port A4



```
HP Switch(config)# debug ip rip database include port A4

HP Switch(config)# show debug

 Debug Logging

  Destination: Session

  Enabled debug types:
   ip rip database include port A4
   snmp trap include ip 10.10.10.1
```

Figure 231 Example of setting a filter for fatal SSH messages on a VLAN



```
HP Switch(config)# debug ssh fatal include vlan 2

HP Switch(config)# show debug

 Debug Logging

  Destination: Session

  Enabled debug types:
   ip rip database include port A4
   snmp trap include ip 10.10.10.1
   ssh (fatal) include vlan 2
```

Enabling or disabling syslog messaging

Use the `debug destination` command to enable (and disable)syslog messaging on a syslog server or to a CLI session for specified types of debug and Event Log messages.

Syntax:

```
[ no ] debug destination[  logging | session | buffer ]
logging
```

Enables syslog logging to configured syslog servers so that the debug message types specified by the `debug` *`debug-type`* command (see "Debug Messages" on page A-47) are sent.

(Default: Logging disabled)

To configure a syslog server IP address, see “Configuring a syslog server” (page 441).

NOTE: Debug messages from the switches covered in this guide have a debug severity level. Because the default configuration of some syslog servers ignores syslog messages with the debug severity level, ensure that the syslog servers you want to use to receive debug messages are configured to accept the debug level. For more information, see “Operating notes for debug and Syslog” (page 446).

`session`	Enables transmission of event notification messages to the CLI session that most recently executed this command. The session can be on any one terminal emulation device with serial, Telnet, or SSH access to the CLI at the Manager level prompt (`HP Switch#_`). If more than one terminal device has a console session with the CLI, you can redirect the destination from the current device to another device. Do so by executing `debug`

	`destination session` in the CLI on the terminal device on which you now want to display event messages. Event message types received on the selected CLI session are configured with the `debug` *`debug-type`* command.
`buffer`	Enables syslog logging to send the debug message types specified by the `debug` *`debug-type`* command to a buffer in switch memory. To view the debug messages stored in the switch buffer, enter the `show debug buffer` command.

Logging command

At the global configuration level, the `logging`command allows you to enable debug logging on specified syslog servers and select a subset of Event Log messages to send for debugging purposes according to:

- Severity level
- System module

By specifying both a severity level and system module, you can use both configured settings to filter the Event Log messages you want to use to troubleshoot switch or network error conditions.

CAUTION: After you configure a syslog server and a severity level and/or system module to filter the Event Log messages that are sent, if you save these settings to the startup configuration file by entering the `write memory` command, these debug and logging settings are automatically re-activated after a switch reboot or power recycle. The debug settings and destinations configured in your previous troubleshooting session will then be applied to the current session, which may not be desirable.

After a reboot, messages remain in the Event Log and are not deleted. However, after a power recycle, all Event Log messages are deleted.

If you configure a severity level, system module, or both to temporarily filter Event Log messages, be sure to reset the values to their default settings by entering the `no` form of the following commands to ensure that Event Log messages of all severity levels and from all system modules are sent to configured syslog servers:

```
HP Switch(config)# no logging severity
[  debug  |   major  |   error  |   warning  |   info ]

HP Switch(config)# no logging system-module  system-module
```

Configuring a syslog server

Syslog is a client-server logging tool that allows a client switch to send event notification messages to a networked device operating with syslog server software. Messages sent to a syslog server can be stored to a file for later debugging analysis.

To use the syslog feature, you must install and configure a syslog server application on a networked host accessible to the switch. For instructions, see the documentation for the syslog server application.

To configure a syslog service, use the `logging` *`syslog-ip-addr`* command as shown below.

When you configure a syslog server, Event Log messages are automatically enabled to be sent to the server. To reconfigure this setting, use the following commands:

- `debug`

  Specifies additional debug message types (see "Debug Messages" on page A-47).

- `logging`

  Configures the system module or severity level used to filter the Event Log messages sent to configured syslog servers. (See "Configuring the severity level for Event Log messages sent to a syslog server" (page 445) and "Configuring the system module used to select the Event Log messages sent to a syslog server" (page 445).)

To display the currently configured syslog servers as well as the types of debug messages and the severity-level and system-module filters used to specify the Event Log messages that are sent, enter the `show debug` command (See "Debug/syslog configuration commands" (page 428)).

Syntax:

```
[ no ] logging  syslog-ip-addr
```

Enables or disables syslog messaging to the specified IP address. You can configure up to six addresses. If you configure an address when none are already configured, this command enables destination logging (syslog) and the Event debug type. Therefore, at a minimum, the switch begins sending Event Log messages to configured syslog servers. The ACL, IP-OSPF, and/or IP-RIP message types are also sent to the syslog servers if they are currently enabled as debug types. (See "Debug Messages" on page A-47.)

`no logging`	Removes all currently configured syslog logging destinations from the running configuration. Using this form of the command to delete the only remaining syslog server address disables debug destination logging on the switch, but the default Event debug type does not change.
`no logging` *`syslog-ip-address`*	Removes only the specified syslog logging destination from the running configuration. Removing all configured syslog destinations with the `no logging` command (or a specified syslog server destination with the `no logging` *`syslog-ip-address`* command) does not delete the syslog server IP addresses stored in the startup configuration.

Deleting syslog addresses in the startup configuration

Enter a `no logging` command followed by the `write memory` command.

Verifying the deletion of a syslog server address

Display the startup configuration by entering the `show config` command.

Blocking the messages sent to configured syslog servers from the currently configured debug message type

Enter the `no debug` *`debug-type`* command. (See "Debug Messages" on page A-47.)

Disabling syslog logging on the switch without deleting configured server addresses

Enter the `no debug destination logging` command. Note that, unlike the case in which no syslog servers are configured, if one or more syslog servers are already configured and syslog messaging is disabled, configuring a new server address does not re-enable syslog messaging. To re-enable syslog messaging, you must enter the `debug destination logging` command.

Sending logging messages using TCP

Syntax:

```
[ no ] logging ip-addr [ udp 1024-49151 | tcp 1024-49151 ]
```

Allows the configuration of the UDP or TCP transport protocol for the transmission of logging messages to a syslog server.

Specifying a destination port with UDP or TCP is optional.

Default ports: UDP port is 514

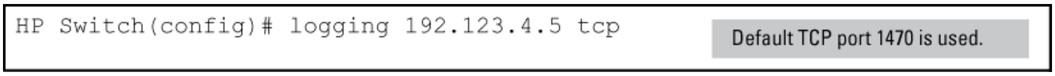
TCP port is 1470

Default Transport Protocol: UDP

Because TCP is a connection-oriented protocol, a connection must be present before the logging information is sent. This helps ensure that the logging message will reach the syslog server. Each configured syslog server needs its own connection. You can configure the destination port that is used for the transmission of the logging messages.

Examples

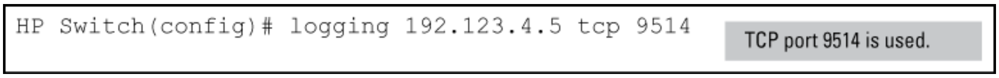
Figure 232 Configuring UDP for logging message transmission using the default port



```
HP Switch(config)# logging 192.123.4.5 tcp
```

Default TCP port 1470 is used.

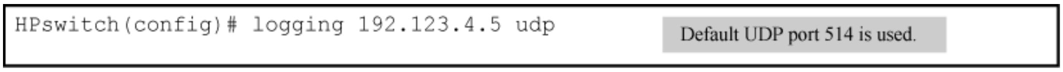
Figure 233 Configuring TCP for logging message transmission using a specified port



```
HP Switch(config)# logging 192.123.4.5 tcp 9514
```

TCP port 9514 is used.

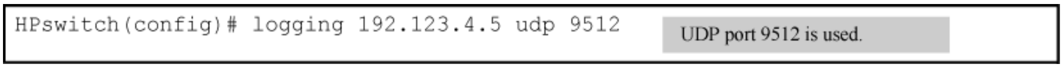
Figure 234 Configuring UDP for logging message transmission using the default port



```
HPswitch(config)# logging 192.123.4.5 udp
```

Default UDP port 514 is used.

Figure 235 Configuring UDP for logging message transmission using a specified port



```
HPswitch(config)# logging 192.123.4.5 udp 9512
```

UDP port 9512 is used.

Syntax:

```
[ no ] logging facility  facility-name
```

The logging facility specifies the destination subsystem used in a configured syslog server. (All configured syslog servers must use the same subsystem.) HP recommends the default (user) subsystem unless your application specifically requires another subsystem. Options include:

`user`	(default) Random user-level messages
`kern`	Kernel messages
`mail`	Mail system
`daemon`	System daemons
`auth`	Security/authorization messages

`syslog`	Messages generated internally by syslog
`lpr`	Line-printer subsystem
`news`	Netnews subsystem
`uucp`	uucp subsystem
`cron`	cron/at subsystem
`sys9`	cron/at subsystem
`sys10 - sys14`	Reserved for system use
`local10 - local17`	Reserved for system use

Use the `no` form of the command to remove the configured facility and reconfigure the default (user) value.

For a list of supported HP switches, see the Note on page A-41

Adding a description for a Syslog server

You can associate a user-friendly description with each of the IP addresses (IPv4 only) configured for syslog using the CLI or SNMP.

CAUTION: Entering the `no logging` command removes ALL the syslog server addresses without a verification prompt.

NOTE: The HP enterprise MIB hpicfSyslog.mib allows the configuration and monitoring of syslog for SNMP (RFC 3164 supported).

The CLI command is:

Syntax:

```
logging ip-addr [control-descr  text_string ]
no logging ip-addr [control-descr]
```

An optional user-friendly description that can be associated with a server IP address. If no description is entered, this is blank. If *`text_string`* contains white space, use quotes around the string. IPv4 addresses only.

Use the `no` form of the command to remove the description. Limit: 255 characters

NOTE: To remove the description using SNMP, set the description to an empty string.

Example

Example 74 `logging` command with a control description

```
HP Switch(config)# logging 10.10.10.2 control-descr syslog_one
```

Adding a priority description

This description can be added with the CLI or SNMP. The CLI command is:

Syntax:

```
logging priority-descr text_string
no logging priority-descr
```

Provides a user-friendly description for the combined filter values of `severity` and `system module`. If no description is entered, this is blank.

If *text_string* contains white space, use quotes around the string.

Use the no form of the command to remove the description.

Limit: 255 characters

Example

Example 75 The logging command with a priority description

```
HP Switch(config)# logging priority-descr severe-pri
```

NOTE: A notification is sent to the SNMP agent if there are any changes to the syslog parameters, either through the CLI or with SNMP.

Configuring the severity level for Event Log messages sent to a syslog server

Event Log messages are entered with one of the following severity levels (from highest to lowest):

`Major`	A fatal error condition has occurred on the switch.
`Error`	An error condition has occurred on the switch.
`Warning`	A switch service has behaved unexpectedly.
`Information`	Information on a normal switch event.
`Debug`	Reserved for HP switch internal diagnostic information.

Using the `logging severity` command, you can select a set of Event Log messages according to their severity level and send them to a syslog server. Messages of the selected and higher severity will be sent. To configure a syslog server, see "Configuring a syslog server" (page 441).

Syntax:

```
[ no ] logging severity[  major | error | warning | info |
debug  ]
```

Configures the switch to send all Event Log messages with a severity level equal to or higher than the specified value to all configured Syslog servers.

Default: `debug` (Reports messages of all severity levels.)

Use the no form of the command to remove the configured severity level and reconfigure the default value, which sends Event Log messages of all severity levels to syslog servers.

NOTE: The severity setting does not affect event notification messages that the switch normally sends to the Event Log. All messages remain recorded in the Event Log.

Configuring the system module used to select the Event Log messages sent to a syslog server

Event Log messages contain the name of the system module that reported the event. Using the `logging system-module` command, you can select a set of Event Log messages according to the originating system module and send them to a syslog server.

Syntax:

```
[ no ] logging system-module  system-module
```

Configures the switch to send all Event Log messages being logged from the specified system module to configured syslog servers. (To configure a syslog server, see "Configuring a syslog server" (page 441).)

See Table C-2 (page 416) for the correct value to enter for each system module.

Default: `all-pass` (Reports all Event Log messages.)

Use the `no` form of the command to remove the configured system module value and reconfigure the default value, which sends Event Log messages from all system modules to syslog servers.

You can select messages from only one system module to be sent to a syslog server; you cannot configure messages from multiple system modules to be sent. If you re-enter the command with a different system module name, the currently configured value is replaced with the new one.

NOTE: This setting has no effect on event notification messages that the switch normally sends to the Event Log.

Operating notes for debug and Syslog

- Rebooting the switch or pressing the `Reset` button resets the debug configuration.

Debug option	Effect of a reboot or reset
logging (debug destination)	If syslog server IP addresses are stored in the startup-config file, they are saved across a reboot and the logging destination option remains enabled. Otherwise, the logging destination is disabled.
session (debug destination)	Disabled.
ACL (debug type)	Disabled.
All (debug type)	Disabled.
event (debug type)	If a syslog server IP address is configured in the startup-config file, the sending of Event Log messages is reset to `enabled`, regardless of the last active setting. If no syslog server is configured, the sending of Event Log messages is `disabled`.
IP (debug type)	Disabled.

- Debugcommands do not affect normal message output to the Event Log.

  Using the `debug event` command, you can specify that Event Log messages are sent to the debug destinations you configure (CLI session, syslog servers, or both) in addition to the Event Log.
- Ensure that your syslog servers accept debug messages.

  All syslog messages resulting from a debug operation have a "debug" severity level. If you configure the switch to send debug messages to a syslog server, ensure that the server's syslog application is configured to accept the "debug" severity level. (The default configuration for some syslog applications ignores the "debug" severity level.)
- Duplicate IP addresses are not stored in the list of syslog servers.
- If the default severity value is in effect, all messages that have severities greater than the default value are passed to syslog. For example, if the default severity is "debug," all messages that have severities greater than debug are passed to syslog.
- There is a limit of six syslog servers. All syslog servers are sent the same messages using the same filter parameters. An error is generated for an attempt to add more than six syslog servers.

Diagnostic tools

Port auto-negotiation

When a link LED does not light (indicating loss of link between two devices), the most common reason is a failure of port auto-negotiation between the connecting ports. If a link LED fails to light when you connect the switch to a port on another device, do the following:

1. Ensure that the switch port and the port on the attached end-node are both set to `Auto` mode.
2. If the attached end-node does not have an `Auto` mode setting, you must manually configure the switch port to the same setting as the end-node port. See Chapter 10, "Port Status and Configuration".

Ping and link tests

The ping test and the link test are point-to-point tests between your switch and another IEEE 802.3-compliant device on your network. These tests can tell you whether the switch is communicating properly with another device.

NOTE: To respond to a ping test or a link test, the device you are trying to reach must be IEEE 802.3-compliant.

Ping test

A test of the path between the switch and another device on the same or another IP network that can respond to IP packets (ICMP Echo Requests). To use the `ping` (or `traceroute`) command with host names or fully qualified domain names, see “DNS resolver” (page 463).

Link test

A test of the connection between the switch and a designated network device on the same LAN (or VLAN, if configured). During the link test, IEEE 802.2 test packets are sent to the designated network device in the same VLAN or broadcast domain. The remote device must be able to respond with an 802.2 Test Response Packet.

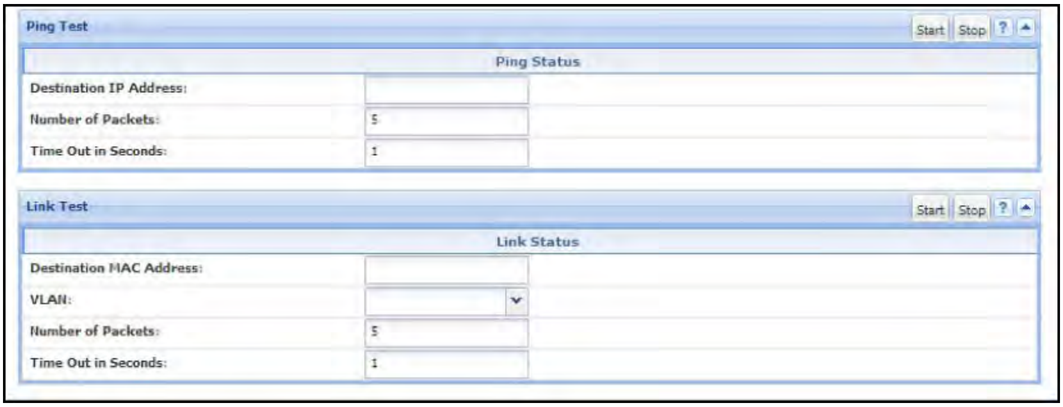
Executing ping or link tests (WebAgent)

To start a ping or link test in the WebAgent:

1. In the navigation pane, click **Troubleshooting**.
2. Click **Ping/Link Test**.
3. Click **Start**.
4. To halt a link or ping test before it concludes, click **Stop**.

For an example of the text screens, see Figure 236 (page 447).

Figure 236 Ping test and link test screen on the WebAgent



Ping Test

Ping Status

Destination IP Address:	
Number of Packets:	5
Time Out in Seconds:	1

Link Test

Link Status

Destination MAC Address:	
VLAN:	
Number of Packets:	5
Time Out in Seconds:	1

Destination IP Address is the network address of the target, or destination, device to which you want to test a connection with the switch. An IP address is in the X.X.X.X format where X is a decimal number between 0 and 255.

Number of Packets to Send is the number of times you want the switch to attempt to test a connection.

Timeout in Seconds is the number of seconds to allow per attempt to test a connection before determining that the current attempt has failed.

Testing the path between the switch and another device on an IP network

The ping test uses ICMP echo requests and ICMP echo replies to determine if another device is alive. It also measures the amount of time it takes to receive a reply from the specified destination. The `ping` command has several extended commands that allow advanced checking of destination availability.

Syntax:

```
ping  ip-address | hostname  [repetitions 1-10000][timeout
1-60][source [ ip-address | vlan-id | loopback 0-7  ]]
[data-size 0 - 65471][data-fill 0-1024][ip-option [
record-route | loose-source-route | strict-source-route |
include-timestamp | include-timestamp-and-address | include
timestamp-from ]][tos 0-255]
```

```
ping6 ipv6-address | hostname  [repetitions 1-10000][timeout
1-60][source [ ip-address | vlan-id | loopback 0-7  ]]
[data-size 0 - 65471][data-fill 0-1024]
```

Sends ICMP echo requests to determine if another device is alive.

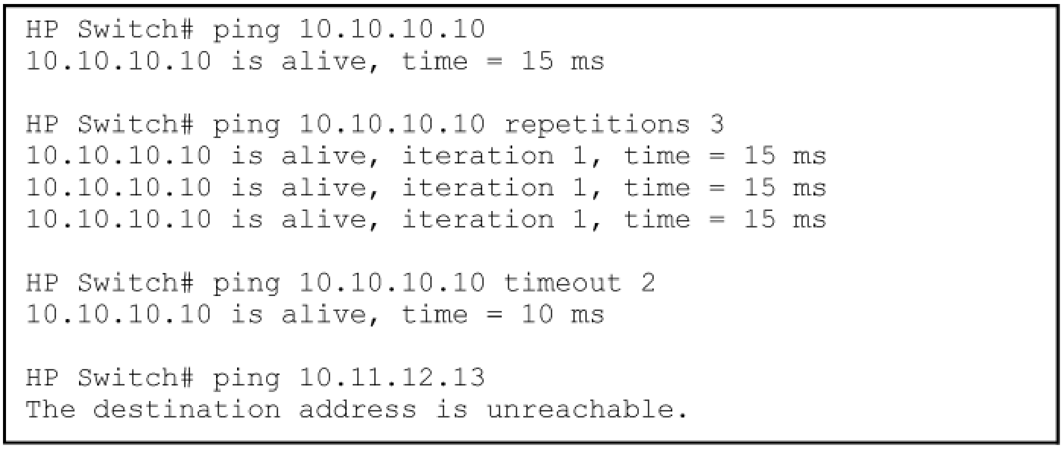
`[ ip-address | hostname ]`	Target IP address or hostname of the destination node being pinged
`repetitions 1-10000`	Number of ping packets sent to the destination address. Default: 1
`timeout 1-60`	Timeout interval in seconds; the ECHO REPLY must be received before this time interval expires for the ping to be successful. Default: 5
`source[ ip-addr | vid | loopback 0-7 ]`	Source IP address, VLAN ID, or loopback address used for the ping. The source IP address must be owned by the router. If a VLAN is specified, the IP address associated with the specified VLAN is used.
`data-size 0-65471`	Size of packet sent. Default: 0 (zero)
`data-fill 0-1024`	The data pattern in the packet. Default: Zero length string
`ip-option`	Specify an IP option, such as loose or strict source routing, or an include-timestamp option: `include-timestamp`: Adds the timestamp option to the IP header. The timestamp displays the amount of travel time to and from a host. Default: 9

	`include-timestamp-and-address`: Records the intermediate router's timestamp and IP address. Default: 4 `include-timestamp-from`: Records the timestamp of the specified router addresses. `loose-source-route` *`IP-addr`*: The `loose-source-route` option prompts for the IP address of each source IP on the path. It allows you to specify the IP addresses that you want the ping packet to go through; the packet may go through other IP addresses as well. `record-route 1-9`: Displays the IP addresses of the interfaces that the ping packet goes through on its way to the destination and on the way back. When specified without loose or strict recording, the source route is not recorded. The source route is automatically recorded when loose or strict source routing is enabled. Default: 9 `strict-source-route` *`IP-addr`*: Restricts the ping packet to only those IP addresses that have been specified and no other addresses.
`tos 0-255`	Specifies the type of service to be entered in the header packet. Default: 0 (zero)

NOTE: For information about `ping6`, see the "IPv6 Configuration Guide" for your switch.

Example

Figure 237 Ping tests



```
HP Switch# ping 10.10.10.10
10.10.10.10 is alive, time = 15 ms

HP Switch# ping 10.10.10.10 repetitions 3
10.10.10.10 is alive, iteration 1, time = 15 ms
10.10.10.10 is alive, iteration 1, time = 15 ms
10.10.10.10 is alive, iteration 1, time = 15 ms

HP Switch# ping 10.10.10.10 timeout 2
10.10.10.10 is alive, time = 10 ms

HP Switch# ping 10.11.12.13
The destination address is unreachable.
```

Halting a ping test before it concludes

Press **[Ctrl] [C]**.

NOTE: To use the `ping` (or `traceroute`) command with host names or fully qualified domain names, see "DNS resolver" (page 463).

Issuing single or multiple link tests

Single or multiple link tests can have varying repetitions and timeout periods. The defaults are:

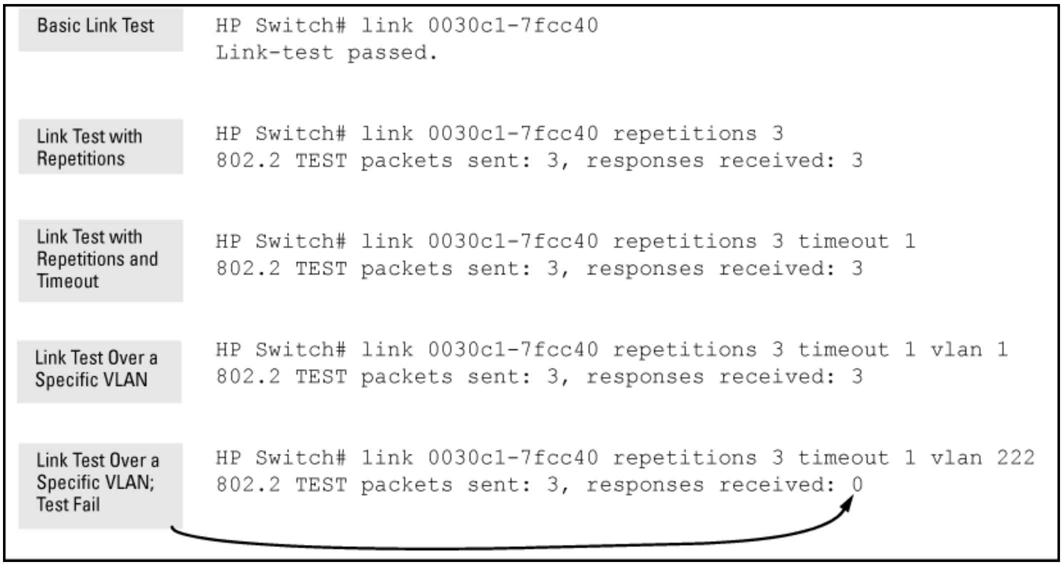
- Repetitions: 1 (1 to 999)
- Timeout: 5 seconds (1 to 256 seconds)

Syntax:

```
link  mac-address  [repetitions 1 - 999 ][timeout 1 - 256 ]
[vlan  vlan-id ]
```

Example

Figure 238 Link tests


Basic Link Test
Link Test with Repetitions
Link Test with Repetitions and Timeout
Link Test Over a Specific VLAN
Link Test Over a Specific VLAN; Test Fail

```
HP Switch# link 0030c1-7fcc40
Link-test passed.

HP Switch# link 0030c1-7fcc40 repetitions 3
802.2 TEST packets sent: 3, responses received: 3

HP Switch# link 0030c1-7fcc40 repetitions 3 timeout 1
802.2 TEST packets sent: 3, responses received: 3

HP Switch# link 0030c1-7fcc40 repetitions 3 timeout 1 vlan 1
802.2 TEST packets sent: 3, responses received: 3

HP Switch# link 0030c1-7fcc40 repetitions 3 timeout 1 vlan 222
802.2 TEST packets sent: 3, responses received: 0
```

Tracing the route from the switch to a host address

This command outputs information for each (router) hop between the switch and the destination address. Note that every time you execute `traceroute`, it uses the same default settings unless you specify otherwise for that instance of the command.

Syntax:

```
traceroute [  ip-address | hostname  ][maxttl 1-255][minttl
1-255][probes 1-5][source [ ip-address | source-vlan vid |
loopback 0-7 ]][dstport 1-34000][srcport 1-34000][ip-option
[ record-route | loose-source-route | strict-source-route |
include-timestamp | include-timestamp-and-address | include
timestamp-from ]][timeout 1-120]
```

Lists the IP address or hostname of each hop in the route, plus the time in microseconds for the traceroute packet reply to the switch for each hop.

`[ip-address	hostname]`	The IP address or hostname of the device to which to send the traceroute.
`[minttl  1-255 ]`	For the current instance of `traceroute`, changes the minimum number of hops allowed for each probe packet sent along the route. • If `minttl` is greater than the actual number of hops, the output includes only the hops at

	and above the `minttl` threshold. (The hops below the threshold are not listed.) • If `minttl` matches the actual number of hops, only that hop is shown in the output. • If `minttl` is less than the actual number of hops, all hops are listed. For any instance of `traceroute`, if you want a `minttl` value other than the default, you must specify that value. (Default: 1)
`[maxttl 1-255 ]`	For the current instance of `traceroute`, changes the maximum number of hops allowed for each probe packet sent along the route. If the destination address is further from the switch than `maxttl` allows, `traceroute` lists the IP addresses for all hops it detects up to the `maxttl` limit. For any instance of `traceroute`, if you want a `maxttl` value other than the default, you must specify that value. (Default: 30)
`[probes 1-5 ]`	For the current instance of `traceroute`, changes the number of queries the switch sends for each hop in the route. For any instance of `traceroute`, if you want a probes value other than the default, you must specify that value. (Default: 3)
`[source ip-addr | vid | loopback 0-7 ]`	The source IPv4 address, VLAN ID, or Loopback address.
`[dstport 1-34000]`	Destination port.
`[srcport 1-34000]`	Source port.
`[ip-option]`	Specify an IP option, such as loose or strict source routing, or an include-timestamp option: `[include-timestamp]`: Adds the timestamp option to the IP header. The timestamp displays the amount of travel time to and from a host. Default: 9 `[include-timestamp-and-address]`: Records the intermediate router's timestamp and IP address. Default: 4 `[loose-source-route IP-addr]`: Prompts for the IP address of each source IP on the path. It allows you to specify the IP addresses that you want the ping packet to go through; the packet may go through other IP addresses as well. `[record-route 1-9]`: Displays the IP addresses of the interfaces that the ping packet goes through on its way to the destination and on the way back. When specified without loose or strict recording, the source route is not recorded. The source route

	is automatically recorded when loose or strict source routing is enabled. Default: 9 `[strict-source-route IP-addr]`: Restricts the ping packet to only those IP addresses that have been specified and no other addresses. `[timeout 1-120 ]`: For the current instance of `traceroute`, changes the timeout period the switch waits for each probe of a hop in the route. For any instance of `traceroute`, if you want a timeout value other than the default, you must specify that value. (Default: 5 seconds)

NOTE: For information about `traceroute6`, see the "IPv6 Configuration Guide" for your switch.

Halting an ongoing traceroute search

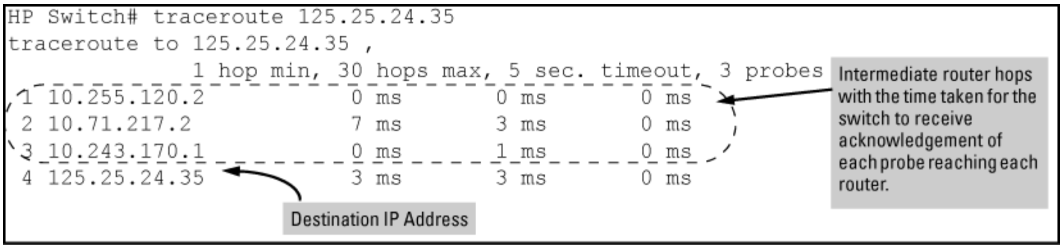
Press the **[Ctrl] [C]** keys.

Examples

A low `maxttl` causes `traceroute` to halt before reaching the destination address

Executing `traceroute` with its default values for a destination IP address that is four hops away produces a result similar to this:

Figure 239 A completed `traceroute` enquiry



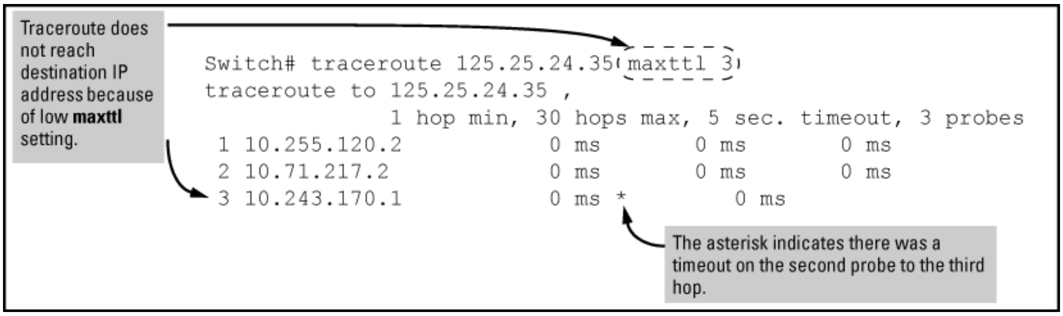
```
HP Switch# traceroute 125.25.24.35
traceroute to 125.25.24.35 ,
                1 hop min, 30 hops max, 5 sec. timeout, 3 probes
  1 10.255.120.2               0 ms          0 ms          0 ms
  2 10.71.217.2                7 ms          3 ms          0 ms
  3 10.243.170.1               0 ms          1 ms          0 ms
  4 125.25.24.35               3 ms          3 ms          0 ms
```

Intermediate router hops with the time taken for the switch to receive acknowledgement of each probe reaching each router.

Destination IP Address

Continuing from the previous example (Figure 239 (page 452)), executing `traceroute` with an insufficient `maxttl` for the actual hop count produces an output similar to this:

Figure 240 Incomplete `traceroute` because of low `maxttl` setting



Traceroute does not reach destination IP address because of low **maxttl** setting.

```
Switch# traceroute 125.25.24.35 maxttl 3
traceroute to 125.25.24.35 ,
                1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.255.120.2             0 ms          0 ms          0 ms
 2 10.71.217.2              0 ms          0 ms          0 ms
 3 10.243.170.1             0 ms *           0 ms
```

The asterisk indicates there was a timeout on the second probe to the third hop.

If a network condition prevents `traceroute` from reaching the destination

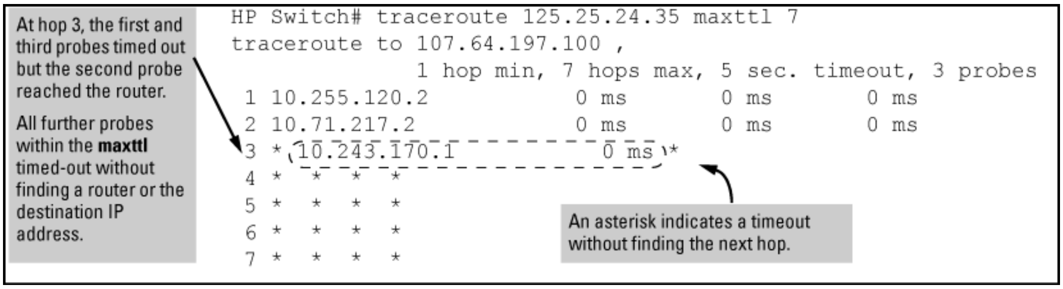
Common reasons for `traceroute` failing to reach a destination include:

- Timeouts (indicated by one asterisk per probe, per hop)
- Unreachable hosts

- Unreachable networks
- Interference from firewalls
- Hosts configured to avoid responding

Executing `traceroute` where the route becomes blocked or otherwise fails results in an output marked by timeouts for all probes beyond the last detected hop. For example, with a maximum hop count of 7 (`maxttl` = 7), where the route becomes blocked or otherwise fails, the output appears similar to this:

Figure 241 Traceroute failing to reach the destination address



```
HP Switch# traceroute 125.25.24.35 maxttl 7
traceroute to 107.64.197.100 ,
              1 hop min, 7 hops max, 5 sec. timeout, 3 probes
 1 10.255.120.2           0 ms        0 ms        0 ms
 2 10.71.217.2            0 ms        0 ms        0 ms
 3 * 10.243.170.1           0 ms *
 4 *    *    *    *
 5 *    *    *    *
 6 *    *    *    *
 7 *    *    *    *
```

At hop 3, the first and third probes timed out but the second probe reached the router.

All further probes within the **maxttl** timed-out without finding a router or the destination IP address.

An asterisk indicates a timeout without finding the next hop.

Viewing Switch Configuration and Operation

In some troubleshooting scenarios, you may need to view the switch configuration to diagnose a problem. The complete switch configuration is contained in a file that you can browse from the CLI using the commands described in this section.

Viewing the startup or running configuration file

Syntax:

```
write terminal
```

Displays the running configuration.

`show config`	Displays the startup configuration.
`show running-config`	Displays the running-config file.

For more information and examples of how to use these commands, see Chapter 6, "Switch Memory and Configuration".

Viewing the configuration file (WebAgent)

To display the running configuration using the WebAgent:

1. In the navigation pane, click **Troubleshooting**.
2. Click **Configuration Report**.
3. Use the right-side scroll bar to scroll through the configuration listing.

Viewing a summary of switch operational data

Syntax:

```
show tech
```

By default, the `show tech` command displays a single output of switch operating and running-configuration data from several internal switch sources, including:

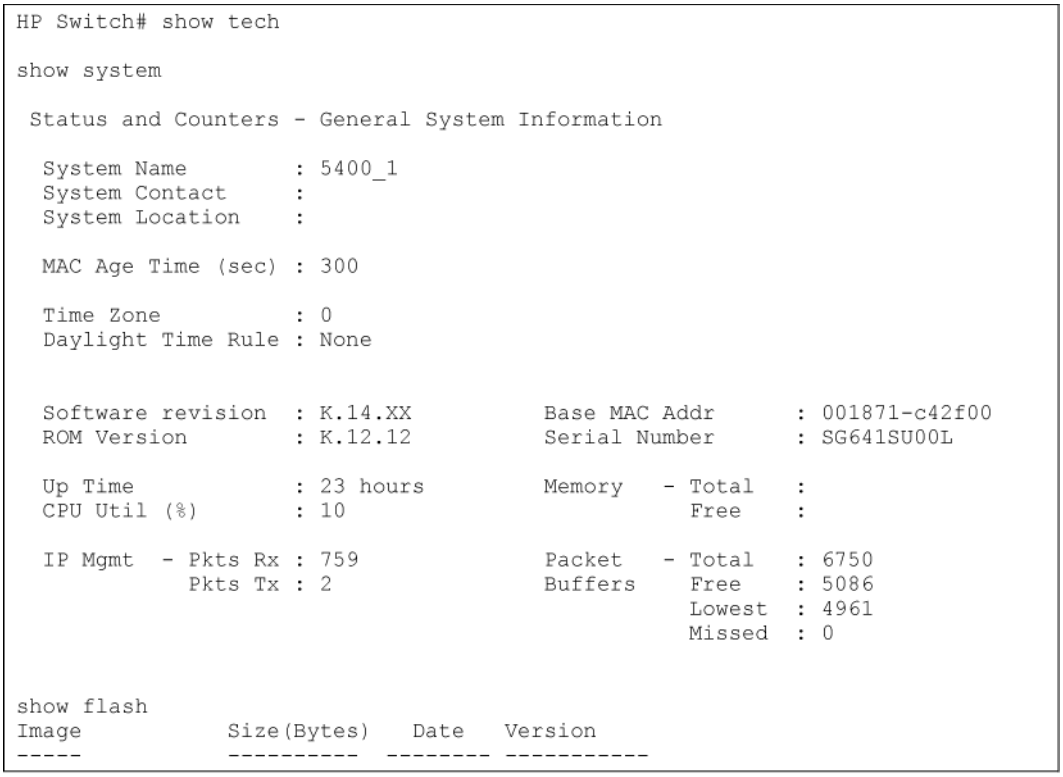
- Image stamp (software version data)
- Running configuration

- Event Log listing
- Boot history
- Port settings
- Status and counters—port status
- IP routes
- Status and counters—VLAN information
- GVRP support
- Load balancing (trunk and LACP)

Example

Figure 242 (page 454) shows sample output from the `show tech` command.

Figure 242 `show tech` command



```
HP Switch# show tech

show system

 Status and Counters - General System Information

  System Name         : 5400_1
  System Contact      :
  System Location     :

  MAC Age Time (sec)  : 300

  Time Zone           : 0
  Daylight Time Rule  : None


  Software revision   : K.14.XX             Base MAC Addr      : 001871-c42f00
  ROM Version         : K.12.12             Serial Number      : SG641SU00L

  Up Time             : 23 hours            Memory    - Total    :
  CPU Util (%)        : 10                              Free     :

  IP Mgmt   - Pkts Rx : 759                 Packet    - Total    : 6750
              Pkts Tx : 2                   Buffers     Free     : 5086
                                                        Lowest   : 4961
                                                        Missed   : 0


show flash
Image            Size(Bytes)   Date    Version
-----            ----------  -------- -----------
```

To specify the data displayed by the `show tech` command, use the `copy show tech` command as described in "Customizing `show tech` command output" (page 455).

Saving `show tech` command output to a text file

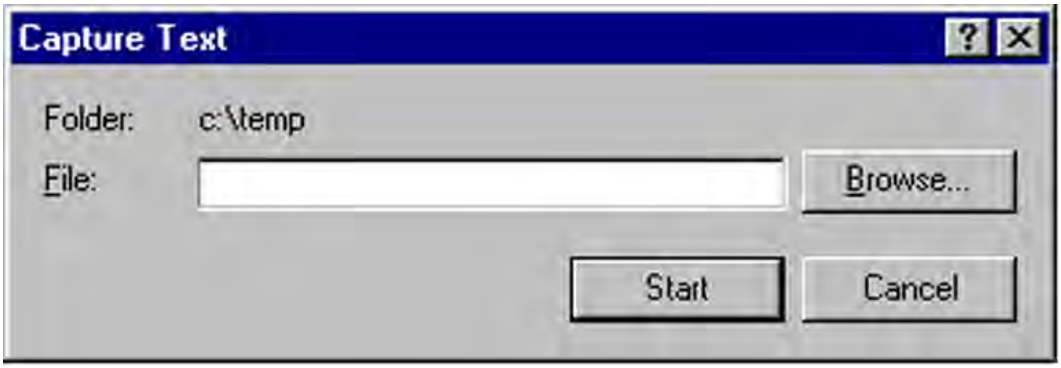
When you enter the `show tech` command, a summary of switch operational data is sent to your terminal emulator. You can use your terminal emulator's text capture features to save the `show tech` data to a text file for viewing, printing, or sending to an associate to diagnose a problem.

For example, if your terminal emulator is the Hyperterminal application available with Microsoft® Windows® software, you can copy the `show tech` output to a file and then use either Microsoft Word or Notepad to display the data. (In this case, Microsoft Word provides the data in an easier-to-read format.)

The following example uses the Microsoft Windows terminal emulator. If you are using a different terminal emulator application, see the documentation provided with the application.

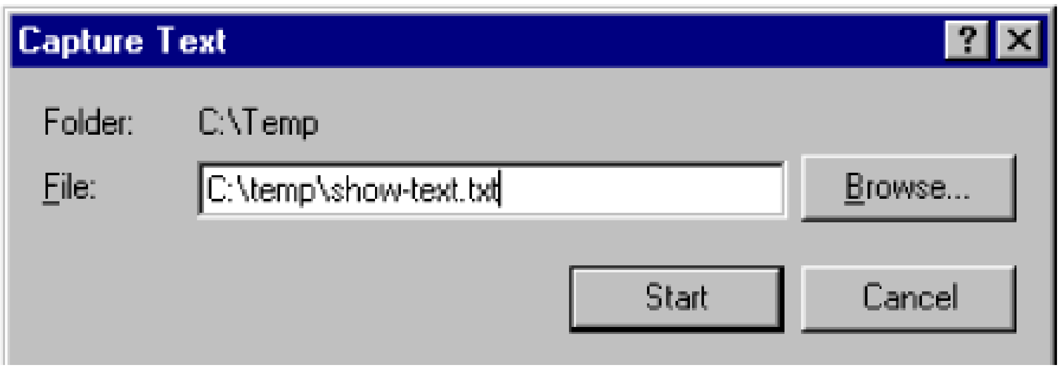
1. In Hyperterminal, click on `TransferCapture Text`...(see Figure 243 (page 455)).

Figure 243 Capture Text window of the Hyperterminal application



2. In the `File` field, enter the path and file name in which you want to store the `show tech` output, as shown in Figure 244 (page 455).

Figure 244 Entering a path and filename for saving `show tech` output



Folder: C:\Temp

File: C:\temp\show-text.txt

3. Click **[Start]** to create and open the text file.
4. From the global configuration context, enter the `show tech` command:

```
HP Switch# show tech
```

The `show tech` command output is copied into the text file and displayed on the terminal emulator screen. When the command output stops and displays the following, press the Space bar to display and copy more information.

```
-- MORE --
```

The CLI prompt appears when the command output finishes.

5. Click on
`Transfer | Capture Text | Stop`
in HyperTerminal to stop copying data and save the text file.

If you do not stop HyperTerminal from copying command output into the text file, additional unwanted data can be copied from the HyperTerminal screen.

6. To access the file, open it in Microsoft Word, Notepad, or a similar text editor.

Customizing `show tech` command output

Use the `copy show tech` command to customize the detailed switch information displayed with the `show tech` command to suit your troubleshooting needs.

To customize the information displayed with the `show tech` command:

1. Determine the information that you want to gather to troubleshoot a problem in switch operation.

2. Enter the `copy show tech` command to specify the data files that contain the information you want to view.

Syntax:

```
copy source show- tech
```

Specifies the operational and configuration data from one or more source files to be displayed by the `show tech` command. Enter the command once for each data file that you want to include in the display.

Default: Displays data from all source files, where *`source`* can be any one of the following values:

`command-output "`*`command`*` "`	Includes the output of a specified command in `show-tech` command output. Enter the command name between double-quotation marks, for example, `copy "show system" show-tech`.

`crash-data [ `*`slot-id`*` | master ]`
`:`
	Includes the crash data from all management and interface modules in `show tech` command output.
	To limit the amount of crash data displayed, specify an installed module or management modules, where:
	• `slot-id`: Includes the crash data from an installed module. Valid slot IDs are the letters a through `h`.
	• `master`: Includes the crash data from both management modules.

`crash-log [ `*`slot-id`*` | master ]`
`:`
	Includes the crash logs from all management and interface modules in `show tech` command output.
	To limit the amount of crash-log data displayed, specify an installed module or management modules, where:
	`slot-id`: Includes the crash log from an installed module. Valid slot IDs are the letters a through `h`.
	`master`: Includes the crash log from both management modules.

`event-log`	Copies the contents of the Event Log to `show tech` command output.
`running-config`	Includes the contents of the running configuration file in `show tech` command output
`startup-config`	Includes the contents of the startup configuration file in `show tech` command output.

`tftp config  startup-config | running-config`
`ip-addr``  `*`remote-file`*` [  pc | unix ]`
	Downloads the contents of a configuration file from a remote host to `show tech` command output, where:
	`ip-addr`: Specifies the IP address of the remote host device.
	`remote-file`: Specifies the pathname on the remote host for the configuration file whose contents you want to include in the command output.
	`pcunix`: Specifies whether the remote host is a DOS-based PC or UNIX workstation.

	For more information on using `copy tftp` commands, see the "File Transfers" appendix.
`usb config  startup-config` *`filename`* ` | command-file` *`acl-filename.txt`*	Copies the contents of a configuration file or ACL command file from a USB flash drive to `show tech` command output, where: `startup-config` *`filename`* : Specifies the name of a startup configuration file on the USB drive. `command-file` *`acl-filename.txt`* : Specifies the name of an ACL command file on the USB drive. For more information on using `copy usb` commands, see the "File Transfers" appendix.
`xmodem config  startup-config | config` *`filename`* ` | command-file` *`acl-filename.txt`* `[ pc | unix ]`	Copies the contents of a configuration file or ACL command file from a serially connected PC or UNIX workstation to `show tech` command output, where: `startup-config`: Specifies the name of the startup configuration file on the connected device. `config` *`filename`* : Specifies the pathname of a configuration file on the connected device. `command-file` *`acl-filename.txt`* : Specifies the pathname of an ACL command file on the connected device. `pcunix`: Specifies whether the connected device is a DOS-based PC or UNIX workstation. For more information on using `copy xmodem` commands, see the "File Transfers" appendix.

Viewing more information on switch operation

Use the following commands to display additional information on switch operation for troubleshooting purposes.

Syntax:

```
show boot-history
```

Displays the crash information saved for each management module on the switch [see "Displaying Saved Crash Information" in the "Redundancy (Switch 8212zl)" chapter].

```
show history
```

Displays the current command history. This command output is used for reference or when you want to repeat a command (See “Displaying the information you need to diagnose problems” (page 460)).

```
show system-information
```

Displays globally configured parameters and information on switch operation (see "CLI: Viewing and Configuring System Information" in the "Interface Access and System Information" chapter).

```
show version
```

Displays the software version currently running on the switch and the flash image from which the switch booted (primary or secondary). For more information, see "Displaying Management Information" in the "Redundancy (Switch 8212zl)" chapter.

`show interfaces`

Displays information on the activity on all switch ports (see "Viewing Port Status and Configuring Port Parameters" in the "Port Status and Configuration" chapter).

`show interfaces-display`

Displays the same information as the `show interfaces` command and dynamically updates the output every three seconds. Press **Ctrl + C** to stop the dynamic updates of system information. Use the Arrow keys to view information that is off the screen.

Searching for text using pattern matching with `show` command

Selected portions of the output are displayed, depending on the parameters chosen.

Syntax:

`show` *`command option`* `[ include | exclude | begin ]` *`regular expression`*

Uses matching pattern searches to display selected portions of the output from a `show` command. There is no limit to the number of characters that can be matched. Only regular expressions are permitted; symbols such as the asterisk cannot be substituted to perform more general matching.

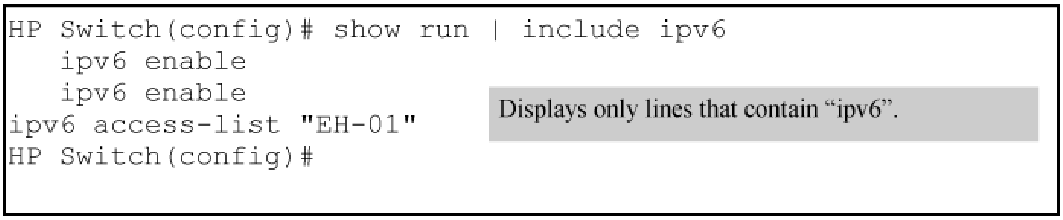
`include`	Only the lines that contain the matching pattern are displayed in the output.
`exclude`	Only the lines that contain the matching pattern are *not* displayed in the output.
`begin`	The display of the output begins with the line that contains the matching pattern.

NOTE: Pattern matching is case-sensitive.

Examples

Below are examples of what portions of the running config file display depending on the option chosen.

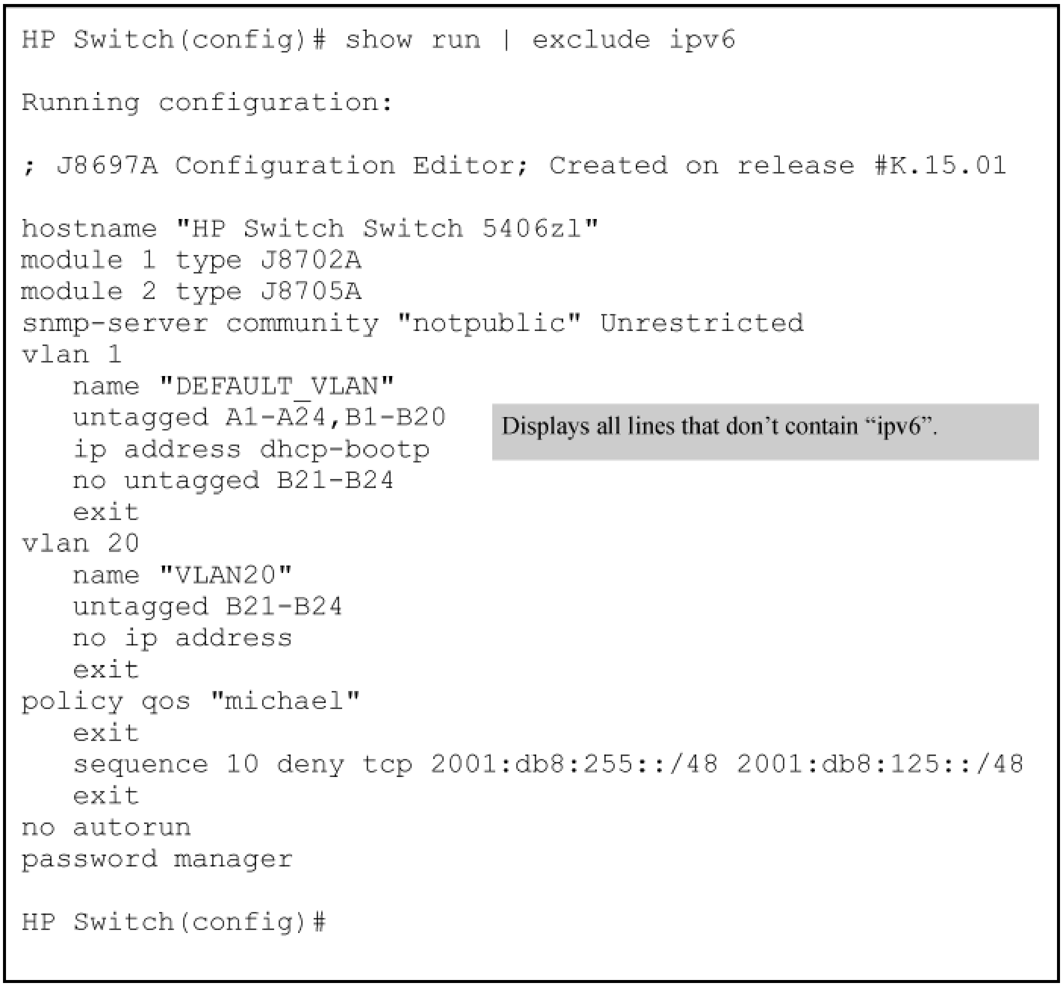
Figure 245 Pattern matching with `include` option



```
HP Switch(config)# show run | include ipv6
   ipv6 enable
   ipv6 enable
ipv6 access-list "EH-01"
HP Switch(config)#
```

Displays only lines that contain “ipv6”.

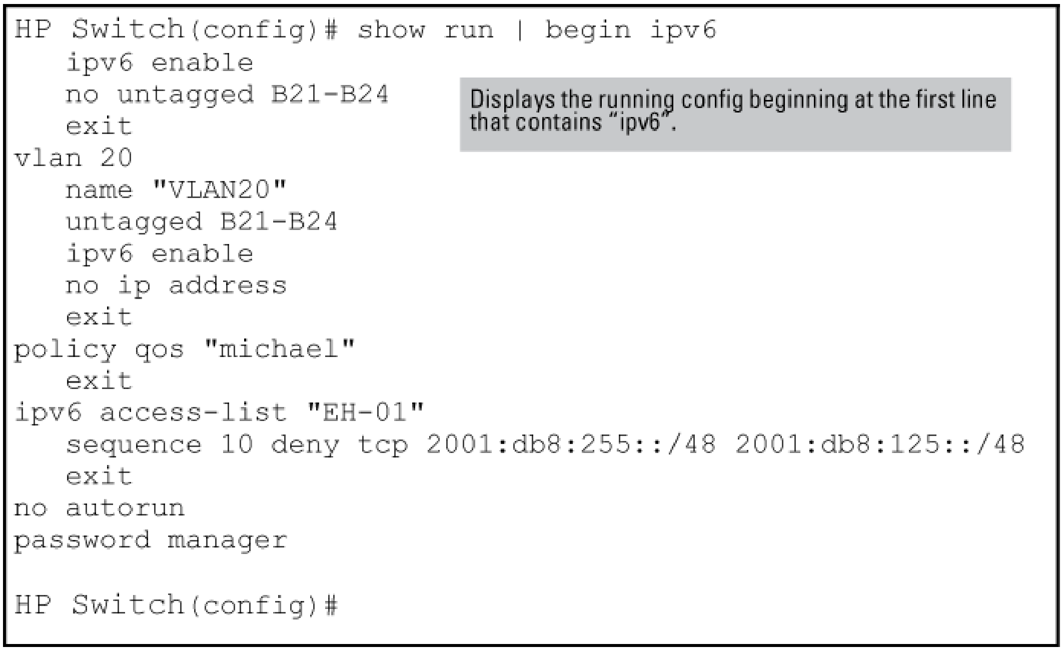
Figure 246 Pattern matching with `exclude` option



```
HP Switch(config)# show run | exclude ipv6

Running configuration:

; J8697A Configuration Editor; Created on release #K.15.01

hostname "HP Switch Switch 5406zl"
module 1 type J8702A
module 2 type J8705A
snmp-server community "notpublic" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A24,B1-B20
   ip address dhcp-bootp
   no untagged B21-B24
   exit
vlan 20
   name "VLAN20"
   untagged B21-B24
   no ip address
   exit
policy qos "michael"
   exit
   sequence 10 deny tcp 2001:db8:255::/48 2001:db8:125::/48
   exit
no autorun
password manager

HP Switch(config)#
```

Displays all lines that don't contain "ipv6".

Figure 247 Pattern matching with `begin` option

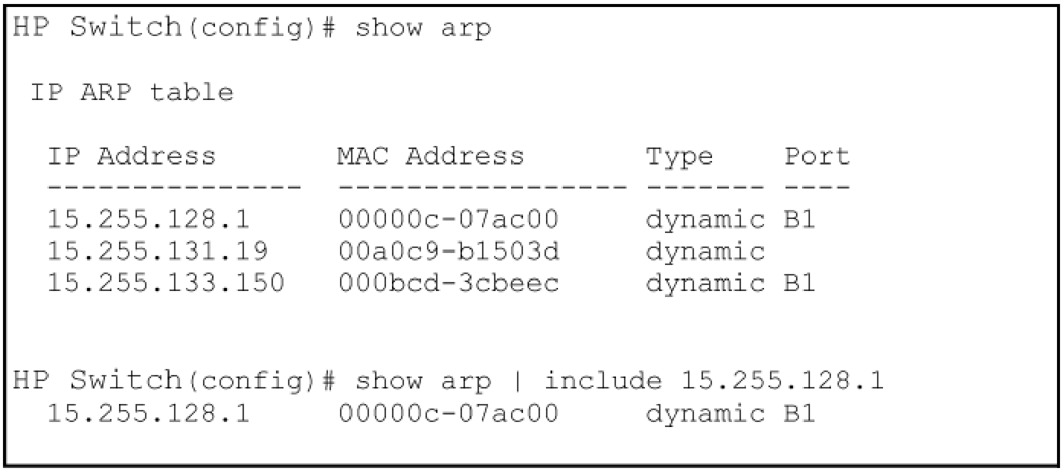


```
HP Switch(config)# show run | begin ipv6
   ipv6 enable
   no untagged B21-B24
   exit
vlan 20
   name "VLAN20"
   untagged B21-B24
   ipv6 enable
   no ip address
   exit
policy qos "michael"
   exit
ipv6 access-list "EH-01"
   sequence 10 deny tcp 2001:db8:255::/48 2001:db8:125::/48
   exit
no autorun
password manager

HP Switch(config)#
```

Displays the running config beginning at the first line that contains "ipv6".

Figure 248 (page 460) is an example of the `show arp` command output, and then the output displayed when the `include` option has the IP address of `15.255.128.1` as the regular expression.

Figure 248 The `show arp` command and pattern matching with the `include` option



```
HP Switch(config)# show arp

 IP ARP table

  IP Address        MAC Address       Type    Port
  ---------------- ----------------- ------- ----
  15.255.128.1      00000c-07ac00     dynamic B1
  15.255.131.19     00a0c9-b1503d     dynamic
  15.255.133.150    000bcd-3cbeec     dynamic B1


HP Switch(config)# show arp | include 15.255.128.1
  15.255.128.1      00000c-07ac00     dynamic B1
```

Displaying the information you need to diagnose problems

Use the following commands in a troubleshooting session to more accurately display the information you need to diagnose a problem. For more information on other CLI practices, see chapter 4, "Using the Command Line Interface (CLI)."

Syntax:

```
alias
```

Creates a shortcut alias name for commonly used commands and command options.

For more information, see "Using a Command Alias" in the "Using the Command Line Interface (CLI)" chapter.

Syntax:

```
kill
```

Terminates a currently running, remote troubleshooting session. Use the `show ip ssh command` to list the current management sessions.

For more information, see "Denying Interface Access by Terminating Remote Management Sessions" in the "Interface Access and System Information" chapter.

Syntax:

```
[ no ] page
```

Toggles the paging mode for `show` commands between continuous listing and per-page listing.

Syntax:

```
repeat
```

Repeatedly executes one or more commands so that you can see the results of multiple commands displayed over a period of time. To halt the command execution, press any key on the keyboard.

For more information, see "Repeating a Command" in the "Using the Command Line Interface (CLI)" chapter.

Syntax:

```
setup
```

Displays the Switch Setup screen from the menu interface.

Restoring the factory-default configuration

As part of your troubleshooting process, it may become necessary to return the switch configuration to the factory default settings. This process

- Momentarily interrupts the switch operation
- Clears any passwords
- Clears the console Event Log
- Resets the network counters to zero
- Performs a complete self test
- Reboots the switch into its factory default configuration, including deleting an IP address

There are two methods for resetting to the factory-default configuration:

- CLI
- `Clear/Reset` button combination

NOTE: HP recommends that you save your configuration to a TFTP server before resetting the switch to its factory-default configuration. You can also save your configuration via Xmodem to a directly connected PC.

Resetting to the factory-default configuration

Using the CLI

This command operates at any level except the Operator level.

Syntax:

```
erase startup-configuration
```

Deletes the startup-config file in flash so that the switch will reboot with its factory-default configuration.

NOTE: The `erase startup-config` command does not clear passwords unless `include-credentials` has been set, at which time this command does erase username/password information and any other credentials stored in the config file. For more information, see the section on "Saving Security Credentials in a Config File" in the *Access Security Guide* for your switch.

Using `Clear/ Reset`

1. Using pointed objects, simultaneously press both the `Reset` and `Clear` buttons on the front of the switch.
2. Continue to press the `Clear` button while releasing the `Reset` button.
3. When the Self Test LED begins to flash, release the `Clear` button.

   The switch then completes its self test and begins operating with the configuration restored to the factory default settings.

Restoring a flash image

The switch can lose its operating system if either the primary or secondary flash image location is empty or contains a corrupted OS file and an operator uses the `erase flash` command to erase a good OS image file from the opposite flash location.

Recovering from an empty or corrupted flash state

Use the switch's console serial port to connect to a workstation or laptop computer that has the following:

- A terminal emulator program with Xmodem capability, such as the HyperTerminal program included in Windows PC software.
- A copy of a good OS image file for the switch.

NOTE: The following procedure requires the use of Xmodem and copies an OS image into primary flash only.

This procedure assumes you are using HyperTerminal as your terminal emulator. If you use a different terminal emulator, you may need to adapt this procedure to the operation of your particular emulator.

1. Start the terminal emulator program.

   Ensure that the terminal program is configured as follows:

• Baud rate: 9600 • No parity • 8 Bits	• 1 stop bit • No flow control

2. Use the `Reset` button to reset the switch.

   The following prompt should then appear in the terminal emulator:

   ```
   Enter h or ? for help.
   =
   ```

3. Because the OS file is large, you can increase the speed of the download by changing the switch console and terminal emulator baud rates to a high speed. For example:

   a. Change the switch baud rate to 115,200 Bps.

   ```
     = sp 115200
   ```

   b. Change the terminal emulator baud rate to match the switch speed:

      i. In HyperTerminal, select `CallDisconnect`.
      ii. Select `FileProperties`.
      iii. Click on **Configure.**
      iv. Change the baud rate to `115200`.
      v. Click on **[OK]**, then in the next window, click on **[OK]** again.
      vi. Select `CallConnect.`
      vii. Press **[Enter]** one or more times to display the = prompt.

4. Start the Console Download utility by entering `do` at the =prompt and pressing **[Enter]**:

   ```
   = do
   ```

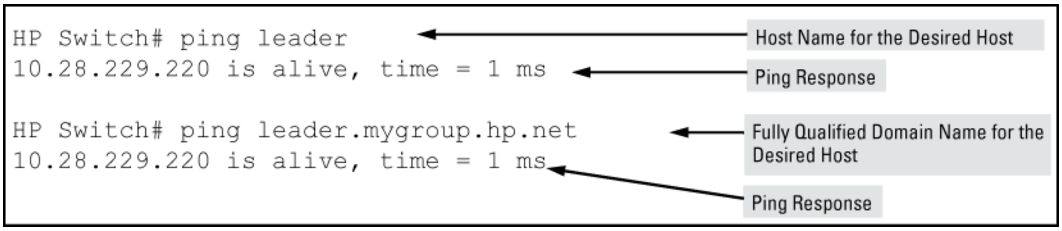
5. You then see this prompt:

   ```
   You have invoked the console download utility.
   Do you wish to continue? (Y/N)>_
   ```

6. At the above prompt:
   a. Enter y (for Yes)
   b. Select `TransferFile` in HyperTerminal.
   c. Enter the appropriate filename and path for the OS image.
   d. Select the `Xmodem` protocol (and not the 1k Xmodem protocol).
   e. Click on **[Send]**.

   If you are using HyperTerminal, you will see a screen similar to the following to indicate that the download is in progress:

Figure 249 Example of Xmodem download in progress



```
HP Switch# ping leader
10.28.229.220 is alive, time = 1 ms

HP Switch# ping leader.mygroup.hp.net
10.28.229.220 is alive, time = 1 ms
```

Host Name for the Desired Host
Ping Response
Fully Qualified Domain Name for the Desired Host
Ping Response

When the download completes, the switch reboots from primary flash using the OS image you downloaded in the preceding steps, plus the most recent startup-config file.

DNS resolver

The domain name system (DNS) resolver is designed for use in local network domains, where it enables the use of a host name or fully qualified domain name with DNS-compatible switch CLI commands. (At software release K.13.01, the DNS-compatible commands include `ping` and `traceroute`.)

Beginning with software release K.13.01, DNS operation supports both IPv4 and IPv6 DNS resolution and multiple, prioritized DNS servers. (For information on IPv6 DNS resolution, see the latest *IPv6 Configuration Guide* for your switch.)

Basic operation

- When the switch is configured with only the IP address of a DNS server available to the switch, a DNS-compatible command, executed with a fully qualified domain name, can reach a device found in any domain accessible through the configured DNS server.
- When the switch is configured with both of the following:
  - The IP address of a DNS server available to the switch
  - The domain suffix of a domain available to the configured DNS server

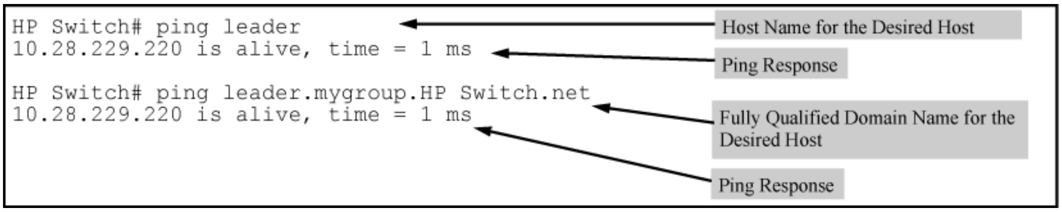
    then:

  - A DNS-compatible command that includes the host name of a device in the same domain as the configured domain suffix can reach that device.
  - A DNS-compatible command that includes a fully qualified domain name can reach a device in any domain that is available to the configured DNS server.

Example

Suppose the switch is configured with the domain suffix mygroup.HP Switch.net and the IP address for an accessible DNS server. If an operator wants to use the switch to ping a target host in this domain by using the DNS name "leader" (assigned by a DNS server to an IP address used in that domain), the operator can use either of the following commands:

Figure 250 Example of using either a host name or a fully qualified domain name



```
HP Switch# ping leader
10.28.229.220 is alive, time = 1 ms

HP Switch# ping leader.mygroup.HP Switch.net
10.28.229.220 is alive, time = 1 ms
```

Host Name for the Desired Host

Ping Response

Fully Qualified Domain Name for the Desired Host

Ping Response

In the proceeding example, if the DNS server's IP address is configured on the switch, but a domain suffix is either not configured or is configured for a different domain than the target host, the fully qualified domain name *must* be used.

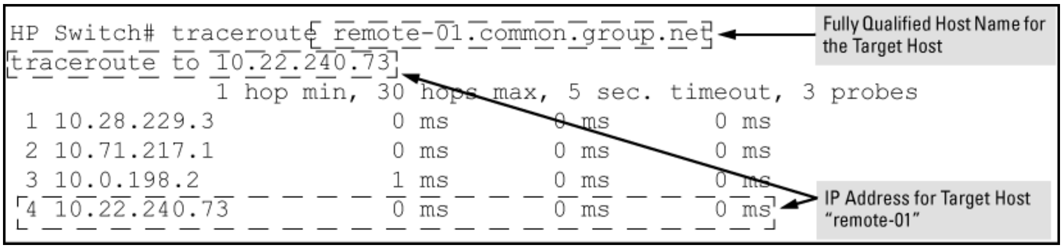
Note that if the target host is in a domain *other than* the domain configured on the switch:

- The host's domain must be reachable from the switch. This requires that the DNS server for the switch must be able to communicate with the DNS servers in the path to the domain in which the target host operates.
- The fully qualified domain name must be used, and the domain suffix must correspond to the domain in which the target host operates, regardless of the domain suffix configured in the switch.

Example

Suppose the switch is configured with the domain suffix mygroup.HP Switch.net and the IP address for an accessible DNS server in this same domain. This time, the operator wants to use the switch to trace the route to a host named "remote-01" in a different domain named common.group.net. Assuming this second domain is accessible to the DNS server already configured on the switch, a `traceroute` command using the target's fully qualified DNS name should succeed.

Figure 251 Example using the fully qualified domain name for an accessible target in another domain



```
HP Switch# traceroute remote-01.common.group.net
traceroute to 10.22.240.73
                1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.28.229.3            0 ms       0 ms       0 ms
 2 10.71.217.1            0 ms       0 ms       0 ms
 3 10.0.198.2             1 ms       0 ms       0 ms
 4 10.22.240.73           0 ms       0 ms       0 ms
```

Fully Qualified Host Name for the Target Host

IP Address for Target Host "remote-01"

Configuring and using DNS resolution with DNS-compatible commands

(At software release K.13.01, the DNS-compatible commands include `ping` and `traceroute`.)

1. Determine the following:
    - The IP address for a DNS server operating in a domain in your network.
    - The priority (1 to 3) of the selected server, relative to other DNS servers in the domain.
    - The domain name for an accessible domain in which there are hosts you want to reach with a DNS-compatible command. (This is the domain suffix in the fully qualified domain name for a given host operating in the selected domain. See "Basic operation" (page 463).) Note that if a domain suffix is not configured, fully qualified domain names can be used to resolve DNS-compatible commands.
    - The host names assigned to target IP addresses in the DNS server for the specified domain.
2. Use the data from the first three bullets in step1 to configure the DNS entry on the switch.
3. Use a DNS-compatible command with the host name to reach the target devices.

Configuring a DNS entry

The switch allows up to two DNS server entries (IP addresses for DNS servers). One domain suffix can also be configured to support resolution of DNS names in that domain by using a host name only. Including the domain suffix enables the use of DNS-compatible commands with a target's host name instead of the target's fully qualified domain name.

Syntax:

```
[ no ] ip dns server-address priority  1 - 3   ip-addr
```

Configures the access priority and IP address of a DNS server accessible to the switch. These settings specify:

- The relative priority of the DNS server when multiple servers are configured
- The IP address of the DNS server

These settings must be configured before a DNS-compatible command can be executed with host name criteria.

The switch supports two prioritized DNS server entries. Configuring another IP address for a priority that has already been assigned to an IP address is not allowed.

To replace one IP address at a given priority level with another address having the same priority, you must first use the `no` form of the command to remove the unwanted address. Also, only one instance of a given server address is allowed in the server list. Attempting to enter a duplicate of an existing entry at a different priority level is not allowed .

To change the priority of an existing server address, use the `no` form of the command to remove the entry, then re-enter the address with the new priority.

The `no` form of the command replaces the configured IP address with the null setting. (Default: null)

Syntax:

```
[ no ]ip dns domain-name  domain-name-suffix
```

This optional DNS command configures the domain suffix that is automatically appended to the host name entered with a DNS-compatible command. When the domain suffix and the IP address for a DNS server that can access that domain are both configured on the switch, you can execute a DNS-compatible command using only the host name of the desired target. (For an example, see Figure 250 (page 464).) In either of the following two instances, you must manually provide the domain identification by using a fully qualified DNS name with a DNS-compatible command:

- If the DNS server IP address is configured on the switch, but the domain suffix is not configured (null).
- The domain suffix configured on the switch is not the domain in which the target host exists.

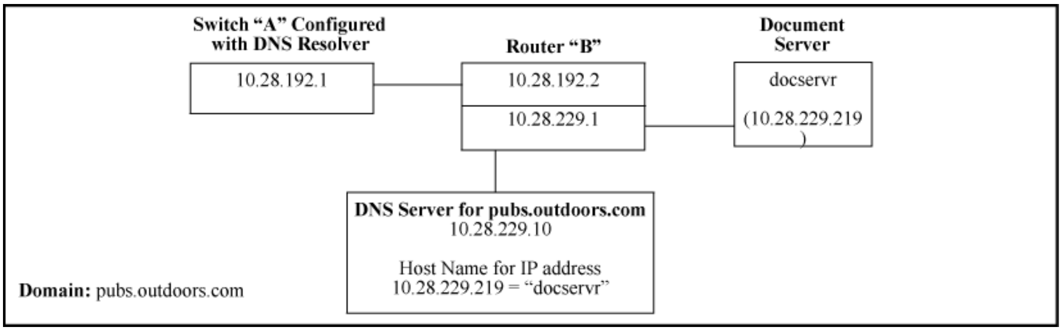
The switch supports one domain suffix entry and three DNS server IP address entries. (See sthe preceding command description.)

The `no` form of the command replaces the configured domain suffix with the null setting. (Default: null)

Using DNS names with ping and traceroute: Example

In the network illustrated in Figure 252 (page 466), the switch at 10.28.192.1 is configured to use DNS names for DNS-compatible commands in the pubs.outdoors.com domain. The DNS server has been configured to assign the host name *docservr* to the IP address used by the document server (10.28.229.219).

Figure 252 Example network domain

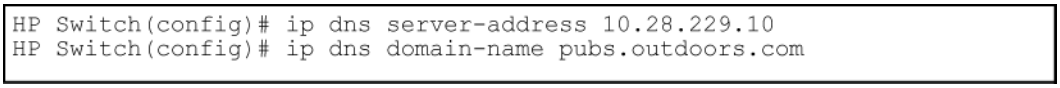

Switch "A" Configured with DNS Resolver
10.28.192.1
Router "B"
10.28.192.2
10.28.229.1
Document Server
docservr
(10.28.229.219)
DNS Server for pubs.outdoors.com
10.28.229.10
Host Name for IP address
10.28.229.219 = "docservr"
Domain: pubs.outdoors.com

Configuring switch "A" with the domain name and the IP address of a DNS server for the domain enables the switch to use host names assigned to IP addresses in the domain to perform `ping` and `traceroute` actions on the devices in the domain. To summarize:

Entity	Identity
DNS server IP address	10.28.229.10
Domain name (and domain suffix for hosts in the domain)	pubs.outdoors.com
Host name assigned to 10.28.229.219 by the DNS server	docservr
Fully qualified domain name for the IP address used by the document server (10.28.229.219)	docservr.pubs.outdoors.com
Switch IP address	10.28.192.1
Document server IP address	10.28.229.219

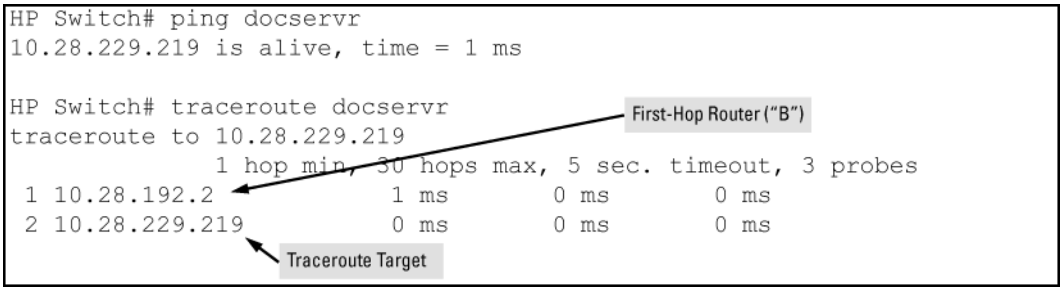
With the above already configured, the following commands enable a DNS-compatible command with the host name `docserver` to reach the document server at 10.28.229.219.

Figure 253 Configuring switch "A" in Figure 252 (page 466) to support DNS resolution



```
HP Switch(config)# ip dns server-address 10.28.229.10
HP Switch(config)# ip dns domain-name pubs.outdoors.com
```

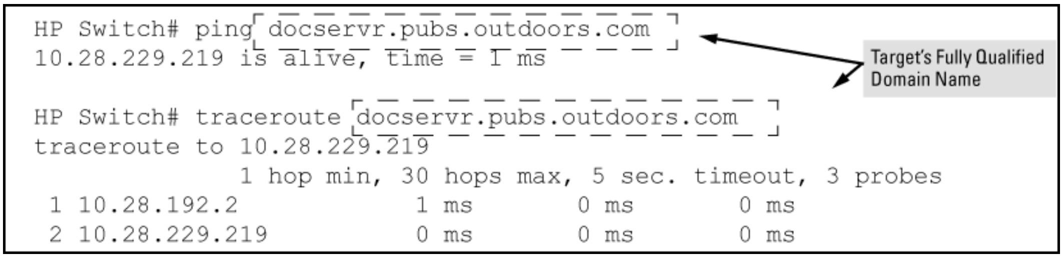
Figure 254 Example of `ping` and `traceroute` execution for the network in Figure 252 (page 466)



```
HP Switch# ping docservr
10.28.229.219 is alive, time = 1 ms

HP Switch# traceroute docservr
traceroute to 10.28.229.219
              1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.28.192.2            1 ms       0 ms       0 ms
 2 10.28.229.219          0 ms       0 ms       0 ms
```

As mentioned under "Basic operation" (page 463), if the DNS entry configured in the switch does not include the domain suffix for the desired target, you must use the target host's fully qualified domain name with DNS-compatible commands. For example, using the document server in Figure 252 (page 466) as a target:

Figure 255 Example of `ping` and `traceroute` execution when only the DNS server IP address is configured



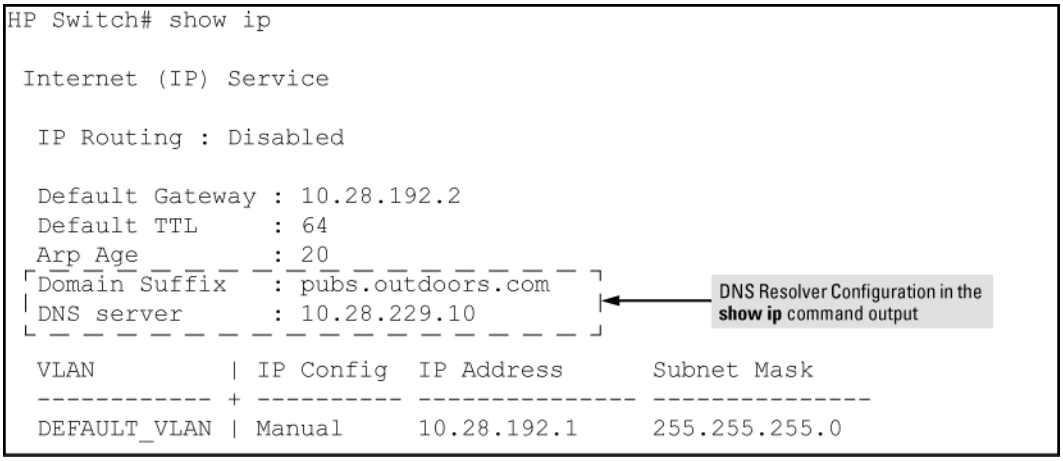
```
HP Switch# ping docservr.pubs.outdoors.com
10.28.229.219 is alive, time = 1 ms

HP Switch# traceroute docservr.pubs.outdoors.com
traceroute to 10.28.229.219
              1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.28.192.2            1 ms        0 ms        0 ms
 2 10.28.229.219          0 ms        0 ms        0 ms
```

Target's Fully Qualified Domain Name

Viewing the current DNS configuration

The `show ip` command displays the current domain suffix and the IP address of the highest priority DNS server configured on the switch, along with other IP configuration information. If the switch configuration currently includes a non-default (non-null) DNS entry, it will also appear in the `show run` command output.

Figure 256 Example of viewing the current DNS configuration



```
HP Switch# show ip

 Internet (IP) Service

  IP Routing : Disabled

  Default Gateway : 10.28.192.2
  Default TTL     : 64
  Arp Age         : 20
  Domain Suffix   : pubs.outdoors.com
  DNS server      : 10.28.229.10

  VLAN         | IP Config  IP Address      Subnet Mask
  ------------ + ---------- --------------- ---------------
  DEFAULT_VLAN | Manual     10.28.192.1     255.255.255.0
```

DNS Resolver Configuration in the **show ip** command output

Operating notes

- Configuring another IP address for a priority that has already been assigned to an IP address is not allowed. To replace one IP address at a given priority level with another address having the same priority, you must first use the no form of the command to remove the unwanted address. Also, only one instance of a given server address is allowed in the server list. Attempting to enter a duplicate of an existing entry at a different priority level is not allowed. To change the priority of an existing server address, use the no form of the command to remove the entry, then re-enter the address with the new priority.
- To change the position of an address already configured with priority *x*, you must first use `no ip dns server-address priority x` *`ip-addr`* to remove the address from the configuration, then use `ip dns server-address priority` *`ip-addr`* to reconfigure the address with the new priority. Also, if the priority to which you want to move an address is already used in the configuration for another address, you must first use the `no` form of the command to remove the current address from the target priority.
- The DNS servers and domain configured on the switch must be accessible to the switch, but it is not necessary for any intermediate devices between the switch and the DNS server to be configured to support DNS operation.
- When multiple DNS servers are configured on the switch, they can reside in the same domain or different domains.
- A DNS configuration must include the IP address for a DNS server that is able to resolve host names for the desired domain. If a DNS server has limited knowledge of other domains, its ability to resolve DNS-compatible command requests is also limited.

- If the DNS configuration includes a DNS server IP address but does not also include a domain suffix, then any DNS-compatible commands should include the target host’s fully qualified domain name.
- Switch-Initiated DNS packets go out through theVLAN having the best route to the DNS server, even if aManagement VLAN has been configured.
- The DNS server address must be manually input. It is not automatically determined viaDHCP.

Event Log messages

Please see the *Event Log Message Reference Guide* for information about Event Log messages.

Locating a switch (Locator LED)

To locate where a particular switch is physically installed, use the `chassislocate` command to activate the blue Locator LED on the switch's front panel.

Syntax:

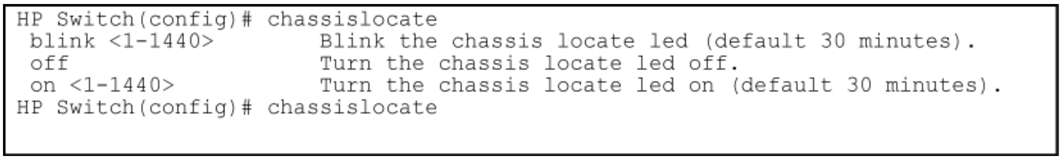
```
chassislocate[ blink | on | off ]
```

Locates a switch by using the blue Locate LED on the front panel.

`blink 1-1440`	Blinks the chassis Locate LED for a specified number of minutes (Default: 30 minutes).
`on 1-1440`	Turns the chassis Locate LED on for a specified number of minutes (Default: 30 minutes).
`off`	Turns the chassis Locate LED off.

Example

Figure 257 Locating a switch with the `chassislocate` command



```
HP Switch(config)# chassislocate
 blink <1-1440>        Blink the chassis locate led (default 30 minutes).
 off                   Turn the chassis locate led off.
 on <1-1440>           Turn the chassis locate led on (default 30 minutes).
HP Switch(config)# chassislocate
```

For redundant management systems, if the active management module failsover, the Locator LED does not remain lit.

D MAC Address Management

Command summary

Table 43 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
`show mac-address [ port-list | mac-addr | vlan vid ]`	Displays port MAC addresses (hexadecimal format),	-	(page 469)	-
`walkmib ifPhysAddress`	Displays the switch's base (default VLAN) MAC address and the addressing for any added VLANs.	-	(page 470)	(page 470)

Overview

The switch assigns MAC addresses in these areas:

- For management functions, one Base MAC address is assigned to the default VLAN (VID = 1). (All VLANs on the switches covered in this guide use the same MAC address.)
- For internal switch operations: One MAC address per port (see "Viewing the port and VLAN MAC addresses" (page 470).

MAC addresses are assigned at the factory. The switch automatically implements these addresses for VLANs and ports as they are added to the switch.

NOTE: The switch's base MAC address is also printed on a label affixed to the switch.

Determining MAC addresses

`Use the CLI` to view the switch's port MAC addresses in hexadecimal format.

`Use the menu interface` to view the switch's base MAC address and the MAC address assigned to any VLAN you have configured on the switch. (The same MAC address is assigned to VLAN1 and all other VLANs configured on the switch.)

NOTE: The switch's base MAC address is used for the default VLAN (VID =1) that is always available on the switch. This is true for dynamic VLANs as well; the base MAC address is the same across all VLANs.

Viewing the MAC addresses of connected devices

Syntax:

```
show mac-address [ port-list | mac-addr | vlan vid ]
```

Lists the MAC addresses of the devices the switch has detected, along with the number of the specific port on which each MAC address was detected.

[*port-list*]	Lists the MAC addresses of the devices the switch has detected, on the specified ports.
[*mac-addr*]	Lists the port on which the switch detects the specified MAC address. Returns the following message if the specified MAC address is not detected on any port in the switch:

	`MAC address  mac-addr  not found.`
`[vlan  vid ]`	Lists the MAC addresses of the devices the switch has detected on ports belonging to the specified VLAN, along with the number of the specific port on which each MAC address was detected.

Viewing the switch's MAC address assignments for VLANs configured on the switch

The Management Address Information screen lists the MAC addresses for:

- Base switch (default VLAN; VID=1)
- Any additional VLANs configured on the switch.

Also, the Base MAC address appears on a label on the back of the switch.

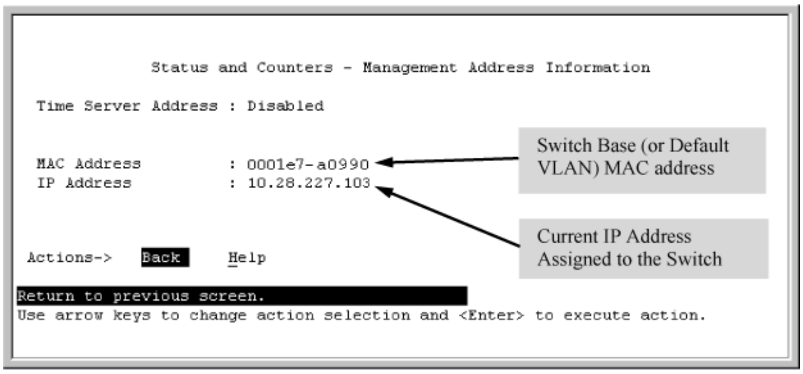
NOTE: The Base MAC address is used by the first (default) VLAN in the switch. This is usually the VLAN named "DEFAULT_VLAN" unless the name has been changed (by using the VLAN Names screen). On the switches covered in this guide, the VID (VLAN identification number) for the default VLAN is always "1," *and cannot be changed*.

- From the Main Menu, select

  1. Status and Counters
  2. Switch Management Address Information

  If the switch has only the default VLAN, the following screen appears. If the switch has multiple static VLANs, each is listed with its address data.

Figure 258 Example of the Management Address Information screen



```
              Status and Counters - Management Address Information

  Time Server Address : Disabled


  MAC Address         : 0001e7-a0990
  IP Address          : 10.28.227.103



 Actions->    Back     Help

Return to previous screen.
Use arrow keys to change action selection and <Enter> to execute action.
```

Switch Base (or Default VLAN) MAC address

Current IP Address Assigned to the Switch

Viewing the port and VLAN MAC addresses

The MAC address assigned to each switch port is used internally by such features as Flow Control and the spanning-tree protocol. Using the `walkmib` command to determine the MAC address assignments for individual ports can sometimes be useful when diagnosing switch operation.

Table 44 Switch series' and their MAC address allocations

Switch series	MAC address allocation
8212zl	The switch allots 24 MAC addresses per slot. For a given slot, if a four-port module is installed, the switch uses the first four MAC addresses in the allotment for that slot, and the remaining 18 MAC addresses are unused.

Table 44 Switch series' and their MAC address allocations *(continued)*

Switch series	MAC address allocation
	If a 24-port module is installed, the switch uses the first 24 MAC addresses in the allotment, and so on.
All Models	The switch's base MAC address is assigned to VLAN (VID) 1 and appears in the `walkmib` listing after the MAC addresses for the ports. (All VLANs in the switch have the same MAC address.)

NOTE: This procedure displays the MAC addresses for all ports and existing VLANs in the switch, regardless of which VLAN you select.

1. If the switch is at the CLI Operator level, use the `enable` command to enter the Manager level of the CLI.
2. Enter the following command to display the MAC address for each port on the switch:

```
HP Switch# walkmib ifPhysAddress
```

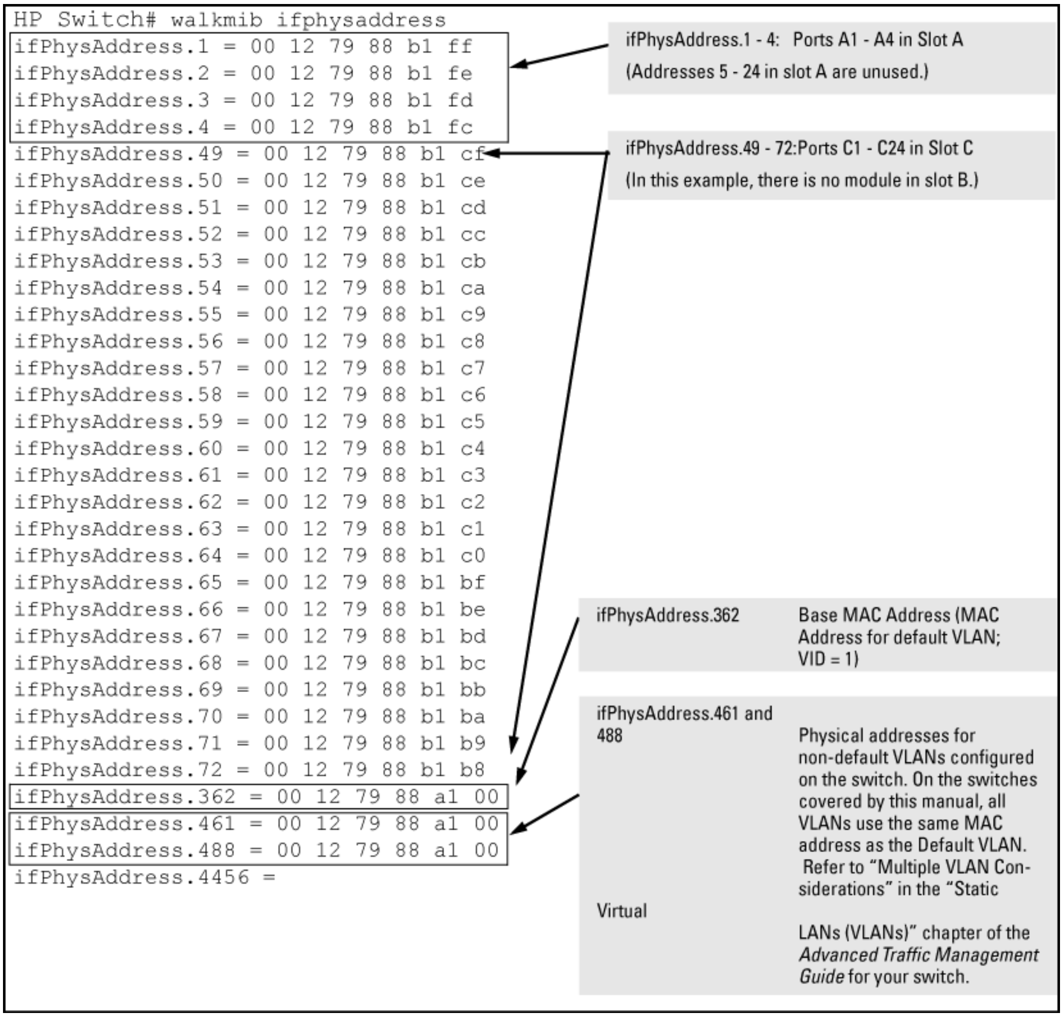
   (The above command is not case-sensitive.)

Example

An HP 8212zl switch with the following module configuration shows MAC address assignments similar to those shown in Figure 259 (page 472):

- A 4-port module in slot A, a 24-port module in slot C, and no modules in slots B and D
- Two non-default VLANs configured

Figure 259 Example of Port MAC address assignments on a switch



```
HP Switch# walkmib ifphysaddress
ifPhysAddress.1 = 00 12 79 88 b1 ff
ifPhysAddress.2 = 00 12 79 88 b1 fe
ifPhysAddress.3 = 00 12 79 88 b1 fd
ifPhysAddress.4 = 00 12 79 88 b1 fc
ifPhysAddress.49 = 00 12 79 88 b1 cf
ifPhysAddress.50 = 00 12 79 88 b1 ce
ifPhysAddress.51 = 00 12 79 88 b1 cd
ifPhysAddress.52 = 00 12 79 88 b1 cc
ifPhysAddress.53 = 00 12 79 88 b1 cb
ifPhysAddress.54 = 00 12 79 88 b1 ca
ifPhysAddress.55 = 00 12 79 88 b1 c9
ifPhysAddress.56 = 00 12 79 88 b1 c8
ifPhysAddress.57 = 00 12 79 88 b1 c7
ifPhysAddress.58 = 00 12 79 88 b1 c6
ifPhysAddress.59 = 00 12 79 88 b1 c5
ifPhysAddress.60 = 00 12 79 88 b1 c4
ifPhysAddress.61 = 00 12 79 88 b1 c3
ifPhysAddress.62 = 00 12 79 88 b1 c2
ifPhysAddress.63 = 00 12 79 88 b1 c1
ifPhysAddress.64 = 00 12 79 88 b1 c0
ifPhysAddress.65 = 00 12 79 88 b1 bf
ifPhysAddress.66 = 00 12 79 88 b1 be
ifPhysAddress.67 = 00 12 79 88 b1 bd
ifPhysAddress.68 = 00 12 79 88 b1 bc
ifPhysAddress.69 = 00 12 79 88 b1 bb
ifPhysAddress.70 = 00 12 79 88 b1 ba
ifPhysAddress.71 = 00 12 79 88 b1 b9
ifPhysAddress.72 = 00 12 79 88 b1 b8
ifPhysAddress.362 = 00 12 79 88 a1 00
ifPhysAddress.461 = 00 12 79 88 a1 00
ifPhysAddress.488 = 00 12 79 88 a1 00
ifPhysAddress.4456 =
```

ifPhysAddress.1 - 4: Ports A1 - A4 in Slot A
(Addresses 5 - 24 in slot A are unused.)

ifPhysAddress.49 - 72:Ports C1 - C24 in Slot C
(In this example, there is no module in slot B.)

ifPhysAddress.362 Base MAC Address (MAC Address for default VLAN; VID = 1)

ifPhysAddress.461 and 488 Physical addresses for non-default VLANs configured on the switch. On the switches covered by this manual, all VLANs use the same MAC address as the Default VLAN. Refer to “Multiple VLAN Considerations” in the “Static Virtual LANs (VLANs)” chapter of the *Advanced Traffic Management Guide* for your switch.

E Monitoring Resources

Displaying current resource usage

Syntax:

```
show  qos | access-list | policy
resources
```

Displays the resource usage of the policy enforcement engine on the switch by software feature. For each type of resource, the amount still available and the amount used by each software feature is shown.

`show resources`	This output allows you to view current resource usage and, if necessary, prioritize and reconfigure software features to free resources reserved for less important features.

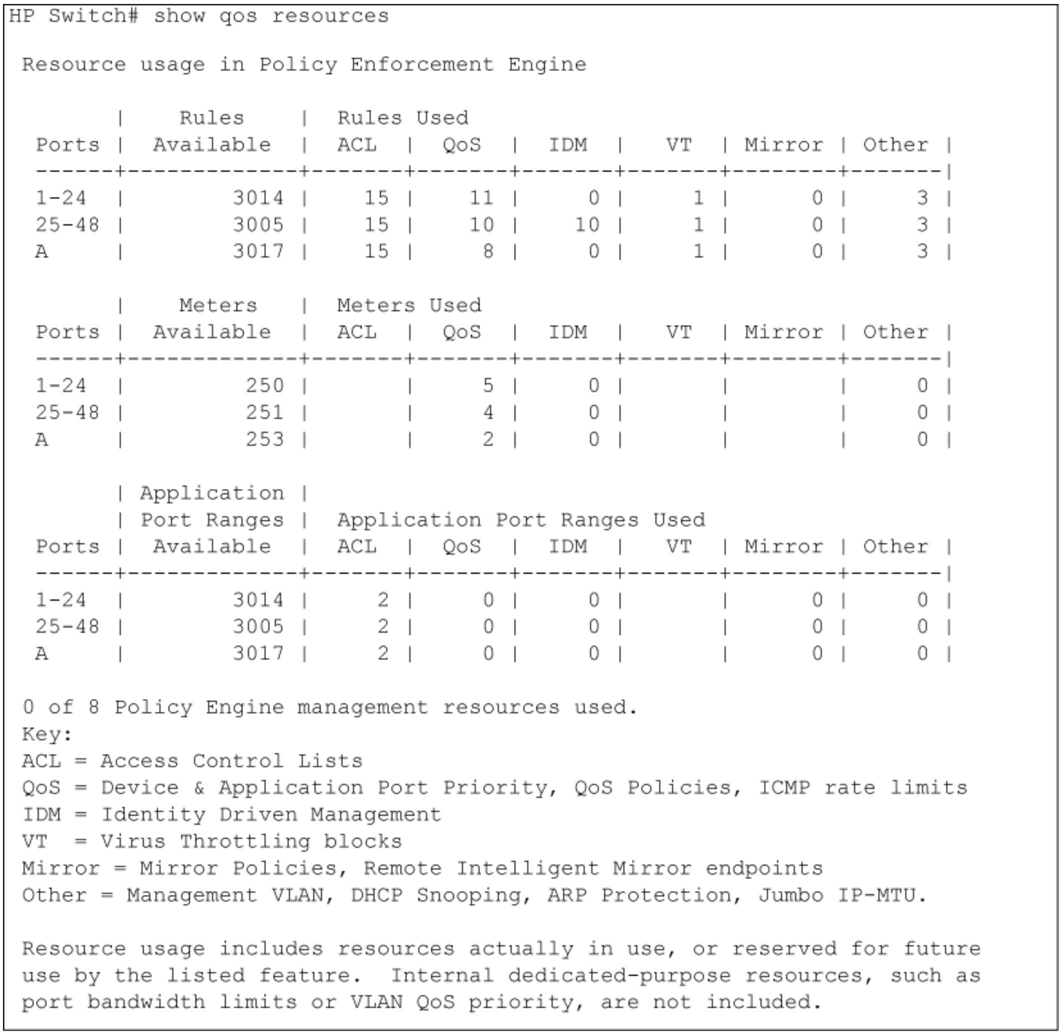
`qos`
`access-list`
`openflow`
`policy`
	Display the same command output and provide different ways to access task-specific information.
	NOTE: See "Viewing OpenFlow Resources" in the *OpenFlow Administrators Guide* for your switch.

Example

Figure A-1shows the resource usage on a 3500yl switch configured for ACLs, QoS, RADIUS-based authentication, and other features:

- The "Rules Used" columns show that ACLs, VT, mirroring, and other features (for example, Management VLAN) have been configured globally or per-VLAN, because identical resource consumption is displayed for each port range in the switch. If ACLs were configured per-port, the number of rules used in each port range would be different.
- The switch is also configured for VT and is either blocking or throttling routed traffic with a high rate-of-connection requests.
- Varying ICMP rate-limiting configurations on ports 1 to 24, on ports 25 to 48, and on slot A, have resulted in different meter usage and different rule usage listed under QoS. Global QoS settings would otherwise result in identical resource consumption on each port range in the switch.
- There is authenticated client usage of IDM resources on ports 25 to 48.

Figure 260 Displaying current QoS resource usage on a series 3500yl switch



```
HP Switch# show qos resources

 Resource usage in Policy Enforcement Engine

       |    Rules     |  Rules Used
  Ports |  Available   |  ACL   |  QoS   |  IDM   |   VT   | Mirror | Other |
  ------+-------------+-------+-------+-------+-------+--------+-------|
  1-24  |        3014 |    15 |    11 |     0 |     1 |      0 |     3 |
  25-48 |        3005 |    15 |    10 |    10 |     1 |      0 |     3 |
  A     |        3017 |    15 |     8 |     0 |     1 |      0 |     3 |

       |    Meters    |  Meters Used
  Ports |  Available   |  ACL   |  QoS   |  IDM   |   VT   | Mirror | Other |
  ------+-------------+-------+-------+-------+-------+--------+-------|
  1-24  |         250 |       |     5 |     0 |       |        |     0 |
  25-48 |         251 |       |     4 |     0 |       |        |     0 |
  A     |         253 |       |     2 |     0 |       |        |     0 |

       | Application |
       | Port Ranges |  Application Port Ranges Used
  Ports |  Available   |  ACL   |  QoS   |  IDM   |   VT   | Mirror | Other |
  ------+-------------+-------+-------+-------+-------+--------+-------|
  1-24  |        3014 |     2 |     0 |     0 |       |      0 |     0 |
  25-48 |        3005 |     2 |     0 |     0 |       |      0 |     0 |
  A     |        3017 |     2 |     0 |     0 |       |      0 |     0 |

 0 of 8 Policy Engine management resources used.
 Key:
 ACL = Access Control Lists
 QoS = Device & Application Port Priority, QoS Policies, ICMP rate limits
 IDM = Identity Driven Management
 VT  = Virus Throttling blocks
 Mirror = Mirror Policies, Remote Intelligent Mirror endpoints
 Other = Management VLAN, DHCP Snooping, ARP Protection, Jumbo IP-MTU.

 Resource usage includes resources actually in use, or reserved for future
 use by the listed feature.  Internal dedicated-purpose resources, such as
 port bandwidth limits or VLAN QoS priority, are not included.
```

Viewing information on resource usage

The switch allows you to view information about the current usage and availability of resources in the Policy Enforcement engine, including the following software features:

- Access control lists (ACL)
- Quality-of-service (QoS), including device and application port priority, ICMP rate-limiting, and QoS policies
- Dynamic assignment of per-port or per-user ACLs and QoS through RADIUS authentication designated as “IDM”, with or without the optional identity-driven management (IDM) application
- Virus throttling (VT) using connection-rate filtering
- Mirroring policies, including switch configuration as an endpoint for remote intelligent mirroring
- Other features, including:
    - Management VLAN
    - DHCP snooping
    - Dynamic ARP protection
    - Jumbo IP-MTU

Policy enforcement engine

The policy enforcement engine is thehardware element in the switch that manages QoS, mirroring, and ACL policies, as well as other software features, using the rules that you configure. Resource usage in the policy enforcement engine is based on how these features are configured on the switch:

- Resource usage by dynamic port ACLs and VT is determined as follows:
    - Dynamic port ACLs configured by a RADIUS server (with or without the optional IDM application) for an authenticated client determine the current resource consumption for this feature on a specified slot. When a client session ends, the resources in use for that client become available for other uses.
    - A VT configuration (connection-rate filtering) on the switch does not affect switch resources unless traffic behavior has triggered either a throttling or blocking action on the traffic from one or more clients. When the throttling action ceases or a blocked client is unblocked, the resources used for that action are released.
- When the following features are configured globally or per-VLAN, resource usage is applied across all port groups or all slots with installed modules:
    - ACLs
    - QoS configurations that use the following commands:
        - QoS device priority (IP address) through the CLI using the `qos device-priority` command
        - QoS application port through the CLI using `qos tcp-port` or `qos udp-port`
        - VLAN QoS policies through the CLI using `service-policy`
    - Management VLAN configuration
    - DHCP snooping
    - Dynamic ARP protection
    - Remote mirroring endpoint configuration
    - Mirror policies per VLAN through the CLI using `monitor service`
    - Jumbo IP-MTU
- When the following features are configured per-port, resource usage is applied only to the slot or port group on which the feature is configured:
    - ACLs or QoS applied per-port or per-user through RADIUS authentication
    - ACLs applied per-port through the CLI using the `ip access-group` or `ipv6 traffic-filter` commands
    - QoS policies applied per port through the CLI using the `service-policy`command
    - Mirror policies applied per-port through the CLI using the `monitor all service` and `service-policy`commands
    - ICMP rate-limiting through the CLI using the `rate-limit icmp`command
    - VT applied to any port (when a high-connection-rate client is being throttled or blocked)

Usage notes for `show resources` output

- A 1:1 mapping of internal rules to configured policies in the switch does not necessarily exist. As a result, displaying current resource usage is the most reliable method for keeping track of available resources. Also, because some internal resources are used by multiple features, deleting a feature configuration may not increase the amount of available resources.
- Resource usage includes resources actually in use or reserved for future use by the listed features.

- "Internal dedicated-purpose resources" include the following features:
  - Per-port ingress and egress rate limiting through the CLI using `rate-limit in/out`
  - Per-port ingress and egress broadcast rate limiting through the CLI using `rate-limit bcast/mcast`
  - Per-port or per-VLAN priority or DSCP through the CLI using `qos priority` or `qos dscp`
  - Per protocol priority through the CLI using `qos protocol`
- For chassis products (for example, the 5400zl or 8212zl switches), 'slots' are listed instead of 'ports,' with resources shown for all installed modules on the chassis.
- The "Available" columns display the resources available for additional feature use.
- The "IDM" column shows the resources used for RADIUS-based authentication with or without the IDM option.
- "Meters" are used when applying either ICMP rate-limiting or a QoS policy with a rate-limit class action.

When insufficient resources are available

The switch has ample resources for configuring features and supporting:

- RADIUS-authenticated clients (with or without the optional IDMapplication)
- VT and blocking on individual clients.

NOTE: Virus throttling does not operate on IPv6 traffic.

If the resources supporting these features become fully subscribed:

- The current feature configuration, RADIUS-authenticated client sessions, and VT instances continue to operate normally.
- The switch generates anevent log notice to say that current resources are fully subscribed.
- Currently engaged resources must be released before any of the following actions are supported:
  - Modifying currently configured ACLs, IDM, VT, and other software features, such as Management VLAN, DHCP snooping, and dynamic ARP protection.

    You can modify currently configured classifier-base QoS and mirroring policies if a policy has not been applied to an interface. However, sufficient resources must be available when you apply a configured policy to an interface.
  - Acceptance of new RADIUS-based client authentication requests (displayed as a new resource entry for IDM).

    Failure to authenticate a client that presents valid credentials may indicate that insufficient resources are available for the features configured for the client in the RADIUS server. To troubleshoot, check the event log.
  - Throttling or blocking of newly detected clients with high rate-of-connection requests (as defined by the current VT configuration).

    The switch continues to generate Event Log notifications (and SNMP trap notification, if configured) for new instances of high-connection-rate behavior detected by the VT feature.

F Daylight Saving Time on HP Switches

This information applies to the following HP switches:

- 212M
- 224M
- 1600M
- 2400M
- 2424M
- 4000M
- 8000M
- Series 2500
- Series 2510
- Series 2600
- Series 2610
- Series 2800
- Switch 2910
- Series 3400cl
- Series 3500
- Series 3500yl
- Series 4100gl
- Series 4200vl
- Series 5300xl
- Series 5400zl
- Switch 6108
- Switch 6200yl
- Series 6400cl
- Switch 6600
- Series 8200zl
- ProCurve AdvanceStack Switches
- ProCurve AdvanceStack Routers

HP Switches provide a way to automatically adjust the system clock for Daylight Saving Time (DST) changes. To use this feature, define the month and date to begin and to end the change from standard time. In addition to the value "none" (no time changes), there are five pre-defined settings, named:

- Alaska
- Canada and Continental US
- Middle Europe and Portugal
- Southern Hemisphere
- Western Europe

The pre-defined settings follow these rules:

Alaska:

- Begin DST at 2 am on the second Sunday in March.
- End DST at 2 am on the first Sunday in November.

Canada and Continental US:

- Begin DST at 2 am on the second Sunday in March.
- End DST at 2 am on the first Sunday in November.

Middle Europe and Portugal:

- Begin DST at 2 am the first Sunday on or after March 25th.
- End DST at 2 am the first Sunday on or after September 24th.

Southern Hemisphere:

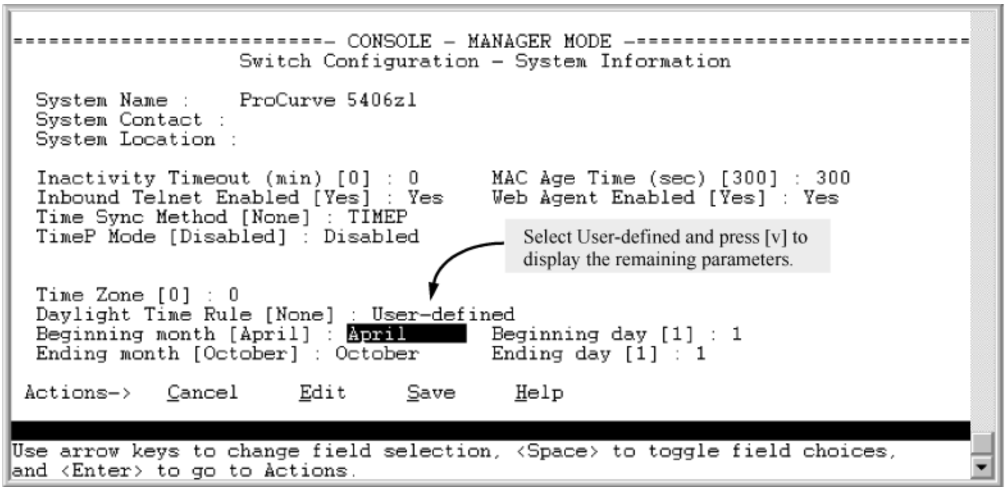
- Begin DST at 2 am the first Sunday on or after October 25th.
- End DST at 2 am the first Sunday on or after March 1st.

Western Europe:

- Begin DST at 2 am the first Sunday on or after March 23rd.
- End DST at 2 am the first Sunday on or after October 23rd.

A sixth option named "User defined" allows you to customize the DST configuration by entering the beginning month and date plus the ending month and date for the time change. The menu interface screen looks like this (all month/date entries are at their default values):

Figure 261 Menu interface with "user-defined" daylight time rule option



```
=========================- CONSOLE - MANAGER MODE -===========================
                   Switch Configuration - System Information

  System Name :     ProCurve 5406zl
  System Contact :
  System Location :

  Inactivity Timeout (min) [0] : 0      MAC Age Time (sec) [300] : 300
  Inbound Telnet Enabled [Yes] : Yes    Web Agent Enabled [Yes] : Yes
  Time Sync Method [None] : TIMEP
  TimeP Mode [Disabled] : Disabled

  Time Zone [0] : 0
  Daylight Time Rule [None] : User-defined
  Beginning month [April] : April       Beginning day [1] : 1
  Ending month [October] : October      Ending day [1] : 1

 Actions->   Cancel     Edit     Save     Help

Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

Select User-defined and press [v] to display the remaining parameters.

Before configuring a "User defined" daylight time rule, it is important to understand how the switch treats the entries. The switch knows which dates are Sundays and uses an algorithm to determine on which date to change the system clock, given the configured "Beginning day" and "Ending day":

- If the configured day is a Sunday, the time changes at 2 am on that day.
- If the configured day is not a Sunday, the time changes at 2 am on the first Sunday after the configured day.

This is true for both the "Beginning day" and the "Ending day."

With that algorithm, you should use the value "1" to represent "first Sunday of the month," and a value equal to "number of days in the month minus 6" to represent "last Sunday of the month." This allows a single configuration for every year, no matter what date is the appropriate Sunday to change the clock.

G Scalability: IP Address, VLAN, and Routing Maximum Values

The following table lists the switch scalability values for the areas of VLANs, ACLs, hardware, ARP, and routing.

Subject	Maximum
IPv4 ACLs	
total named (extended or standard)	Up to 2048 (minus any IPv4 numeric standard or extended ACL assignments and any RADIUS-assigned ACLs)[1]
total numbered standard	Up to 99[1]
total numbered extended	Up to 100[1]
total ACEs in all IPv4 ACLs	Up to 3072[1]
IPv6 ACLs	
total IPv6 ACLs	Up to 2048[1]
total ACEs in all IPv6 ACLs	Up to 3072[1]
Layer-3	
VLANs with at least one IP Address	512
IP addresses per system	2048 IPv4 2048 IPv6[2]
IP addresses per VLAN	32[3]
Static routes (IPv4 and IPv6 combined)	256
IPv4 host hardware table	72 K (8K internal, 64K external)
IPv4 BMP hardware table	2 K
ARP	
ARP entries	25,000
Packets held for ARP resolution	25
Dynamic Routing	
Total routes supported	IPv4 only: 10,000 (including ARP) IPv4 and IPv6: 10 K (IPv4) and 3 K (IPv6)[4] IPv6 only: 5 K[5]
IPv4 Routing Protocol	

Subject	Maximum
RIP interfaces	128
OSPFv2	
Interfaces/subnets	512 (128 active)
Max. areas supported	16
ECMP next hops	4
IPv6 Routing Protocol	
DHCPv6 Helper Addresses	32 unique addresses; multiple instances of same address counts as 1 towards maximum
OSPFv3	
Interfaces/subnets	512 (128 active)
Max. areas supported	16
ECMP next hops	4

[1] Actual availability depends on combined resource usage on the switch. See Appendix E, "Monitoring Resources" (page 473).

[2] These limits apply only to user-configured addresses and not to auto-configured link local and prefix IPv6 addresses. A maximum configuration could support up to 2048 user-configured and 2048 auto-configured IPv6 addresses for a total of 4096.

[3] There can be up to 32 IPv4 and 32 user-configured IPv6 addresses on a single VLAN. In addition, each VLAN is limited to 3 auto-configured prefix-based IPv6 addresses.

[4] Configured as an ABR for OSPF with four IPv4 areas and four IPv6 areas.

[5] Configured as an ABR for OSPF with two IPv6 OSPF areas.

H Switch Licensing

Switch software licensing enables advanced features in certain HP switches. The following table shows the software licenses available for the switches.

License type	Premium (includes OSPF, PIM – sparse mode, PIM – dense mode, VRRP, QinQ)
Switch family	**License product**
3500 and 3500yl	J8993A
5400zl	J8994A
6600	J9305A
8200zl	J9474A

General procedure

The general procedure forinstalling a software license involves several different numbers:

- Registration ID — This number comes with the license you purchase, and represents your right to install the particular type of license on a particular type of switch.
- Hardware ID — This number is provided by the switch that you are licensing, and includes the switch's serial number and an identifier for the feature that you are licensing.
- License key — This number is generated by the My HP Switch portal, based on the registration ID and the hardware ID that you provide. When you install this number into the switch, it enables the feature that you are licensing.

The procedure for installing a licensed feature into a switch is:

1. **Locate the registration ID**. When you purchase a software license, you receive a folded license registration card. The registration ID is located on the inside of the card, in the upper left corner.
2. **Get the switch's hardware ID**. Establish a console connection to the switch CLI and enter Manager level, using the `enable` command if necessary and the switch password if required. For example:

   ```
   HP Switch enable
   HP Switch#
   ```

   From the Manager level, issue the `licenses hardware-id license_type` command. For example:

   ```
   HP Switch# licenses hardware-id premium
   ```

   The CLI returns a hardware ID number. Copy the hardware ID number from the screen (using Ctrl-C) or write it down. (Copying the number is easier and more accurate.) You will enter the number on the My HP Switch portal in the next step.
3. **Get the license key**. Point your Web browser at the My HP Switch portal (http://my.HP Switch.com) and sign in. Click the My Licenses tab, enter the registration ID, and then enter the hardware ID. At the end of the procedure a license key is displayed. (It is also e-mailed to you.) Copy the license key from the screen (using Ctrl-C) or write it down.
4. **Enter the license key into the switch**. On the CLI console, save the configuration of the switch (**write memory**). Then, from a Manager-level prompt, issue a `licenses install premium license-key` command. (The license key number is not case sensitive.) For example:

   ```
   HP Switch# licenses install premium AA000GG000-A-0123ABC-ABCD123-0A2B3C4-0123ABC
   ```

5. Reboot the switch. For example:

   ```
   HP Switch# boot
   ```

   or:

   ```
   HP Switch# reload
   ```

   The licensed features should now be active on the switch.

I Power-Saving Features

Overview

There are several power-saving features that can be configured for the indicated switches and modules. The power-saving features include the ability to:

- Turn slot power on or off
- Turn LED power on or off
- Turn slot auto low power mode on or off
- Use LLDP for Energy Efficient Ethernet

The modules support the power-saving features as indicated in the table below.

Product number	Description	LED power on/off	Slot auto low power mode	Slot power on/off
J8702A	HP Switch zl 24 10/100/1000 PoE Module	Yes	Yes	Yes
J8705A	HP Switch zl 20 Gig-T + 4 mGBIC Module	Yes	Yes	Yes
J8706A	HP Switch zl 24-Port Mini-GBIC Module	Yes	No	Yes
J8707A	HP Switch zl 4-Port 10GbE X2 Module	Yes	No	Yes
J8708A	HP Switch zl 4-Port 10GbE CX4 Module	Yes	No	Yes
J9307A	HP Switch 24-Port 10/100/1000 PoE+ zl Module	Yes	Yes	Yes
J9308A	HP Switch 20-Port 10/100/1000 PoE+/4-Port MiniGBIC zl Module	Yes	Yes	Yes
J9309A	HP Switch 4-Port 10Gbe SFP+ zl Module	Yes	No	Yes
J9478A	HP Switch 24-Port 10/100 PoE+ zl Module	Yes	Yes	Yes

Table 45 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
`[ no ] savepower [module slot-list | all ] [led slot-list | all ] [port-low-pwr [ slot-list | all ]]`	Configures power-saving features.		(page 484)	
`[ no ] savepower led [ slot-list | all ] [timer [ MM/DD[/[YY]YY] HH:MM | now | duration [[HH:MM[recur]]] ]]`	When the timer option is configured, schedules a timer for turning off the chassis LEDs or configured slot LEDs.		(page 485)	
`[ no ] int` *`port-list`* `energy-efficient-ethernet`	Enables EEE for a given port or range of ports.	Enabled	(page 488)	
`[no] lldp config` *`port-list`* `dot3TlvEnable eee_config`	Enables the advertisement of Layer 2 EEE TLVs for a given port or range of ports.	Enabled	(page 490)	

Configuring the power-saving options

Syntax:

```
[ no ] savepower [module  slot-list | all ][led  slot-list
| all ][port-low-pwr [ slot-list | all ]]
```

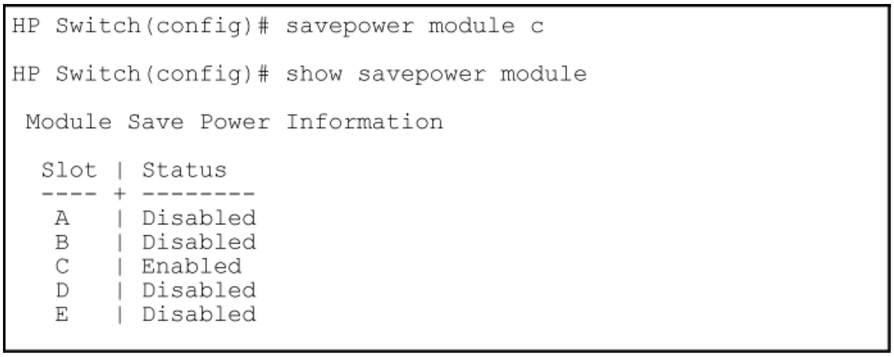
Configures power-saving features.

`module [ slot-list | all ]`	Turns power-saving options on or off for modules.
`led [ slot-list | all ]`	Turns power-saving options on or off for the LEDs for a module, list of modules or all modules.
`port-low-pwr [ slot-list | all ]`	Enables or disables auto power down for slots.

Configuring the savepower module option

The `module` option provides the ability to turn the slot power on or off. If no module is specified, all slots are powered off. You can also specify `all` to turn off the power for all slots. If the command is preceded by no, all the slots are powered on, if off already. (See Figure 262 (page 485).)

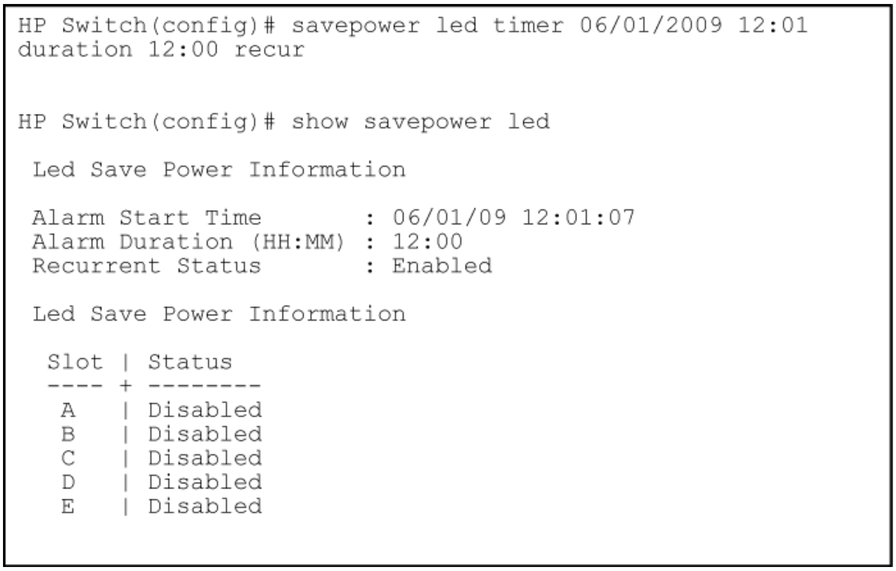
Figure 262 Example of savepower module Command



```
HP Switch(config)# savepower module c

HP Switch(config)# show savepower module

 Module Save Power Information

  Slot | Status
  ---- + --------
   A   | Disabled
   B   | Disabled
   C   | Enabled
   D   | Disabled
   E   | Disabled
```

The `savepower module` command shuts down the specified modules in the order specified in the command. The ports on these modules no longer pass traffic. Any management traffic (SNMP, SSH, Telnet) that passes through these modules is interrupted. It can take up to two minutes to power down all the specified modules. Check the Event Log to see the current status of the module power down. This command applies to PoE/PoE+ modules as well as non-PoE/PoE+ modules.

Figure 263 Example of savepower module all Command



```
HP Switch(config)# savepower led timer 06/01/2009 12:01
duration 12:00 recur


HP Switch(config)# show savepower led

 Led Save Power Information

 Alarm Start Time        : 06/01/09 12:01:07
 Alarm Duration (HH:MM)  : 12:00
 Recurrent Status        : Enabled

 Led Save Power Information

  Slot | Status
  ---- + --------
   A   | Disabled
   B   | Disabled
   C   | Disabled
   D   | Disabled
   E   | Disabled
```

You can verify the status of the `savepower` command by using the `show modules` command or by checking the log messages (for 8200zl and 5400zl switches).

NOTE: If a `savepower module` *`slot-list`* or `savepower module all` command is immediately followed by a `no savepower module` *`slot-list`* or `no savepower module all` command, the first slot in the list is powered down and then brought up.

Configuring the savepower LED option

The savepower LED option provides the ability to turn off specified slot LEDs or all LEDs. You can also configure a timer for turning off the chassis LEDs or the specified slot LEDs.There is one system-wide timer; all the selected slots will have the chassis LEDs turned off for the same amount of time.

Syntax:

```
[ no ] savepower led[  slot-list | all ][timer [ MM/DD[/[YY]YY]
HH:MM | now | duration [HH:MM[recur] ]]
```

If a `slot-list` is specified, the LEDs for that `slot-list` are turned off.

The `all` option can be specified for the `slot-list`. All the chassis LEDs are turned off.

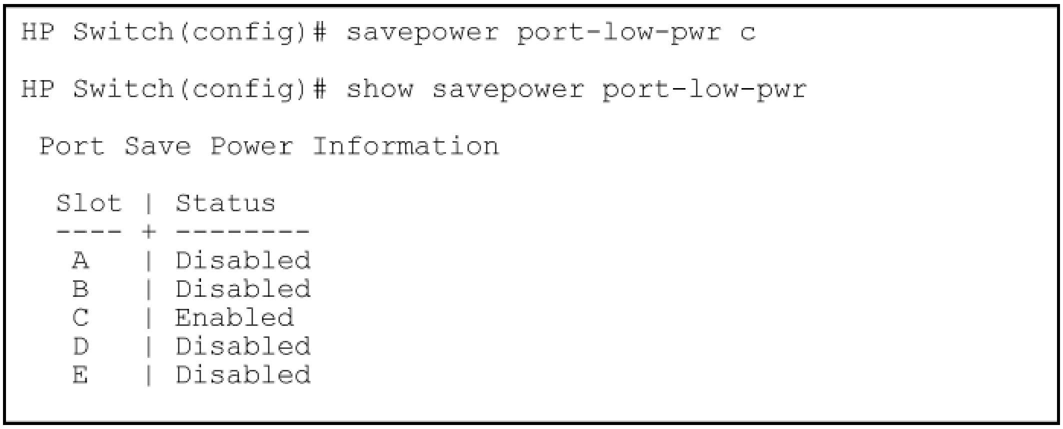
When the timer option is configured, schedules a timer for turning off the chassis LEDs or configured slot LEDs. The LEDs are turned off for the configured time period and duration. (See Figure 264 (page 486).)

`MM/DD[/[YY]YY] HH:MM`	Specifies the date and time to start the timer.
`now`	Instantaneously turns off the LEDs. The configured timer is canceled and all the configured modules go into power-saving mode immediately.
	`duration [HH:]MM`: The amount of time the LEDs remain turned off. (Optional) If the duration value is zero, when the timer starts, the LEDs are turned off indefinitely until the timer is canceled or the command is overridden with another command. Default: 0 (zero)
	`recur`: (Optional) If specified, the LEDs are turned off on a daily basis at the configured time. The `recur` option is ignored if the duration is configured as zero. Default: disabled.

A new command overrides the previous command, regardless of the current state. For example, if a timer is active and new command is given, the currently running timer is canceled and the new timer is scheduled.

The no form of the `savepower led` command cancels any scheduled or running timer and the LEDs are returned to their original state. The `no savepower led all` command turns on all the switch LEDs.

Figure 264 Example of setting a time and duration for savepower led command



```
HP Switch(config)# savepower port-low-pwr c

HP Switch(config)# show savepower port-low-pwr

 Port Save Power Information

  Slot | Status
  ---- + --------
   A   | Disabled
   B   | Disabled
   C   | Enabled
   D   | Disabled
   E   | Disabled
```

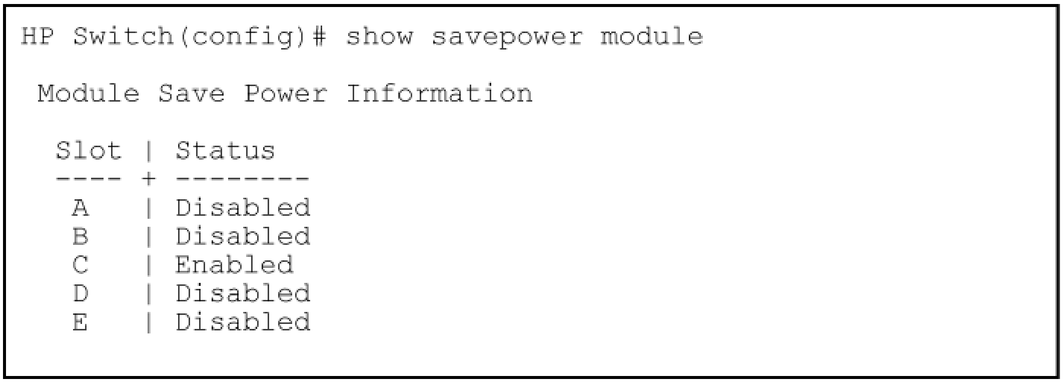
Configuring the savepower port-low-pwr option

The `port-low-pwr`option puts the slots into auto low power mode if they are not linked. If a particular slot is specified, only that slot goes into auto low-power mode. Specifying `savepower port-low-pwr all` puts all the slots into auto low power mode. (See Figure 265 (page 487).)

The ports in low-power mode periodically monitor to determine if the link has become active. If a LAN cable is connected to one of the ports, that port will come out of the low-power mode state after approximately 2 seconds (the monitor period) and enter into normal power mode. The remaining ports continue to be in low-power mode.

The no form of the command puts the specified slot into normal power mode. Entering `no savepower port-low-pwr all` puts all the slots into normal power mode.

Figure 265 Example of `savepower port-low-power` command for slot C



```
HP Switch(config)# show savepower module

 Module Save Power Information

  Slot | Status
  ---- + --------
   A   | Disabled
   B   | Disabled
   C   | Enabled
   D   | Disabled
   E   | Disabled
```

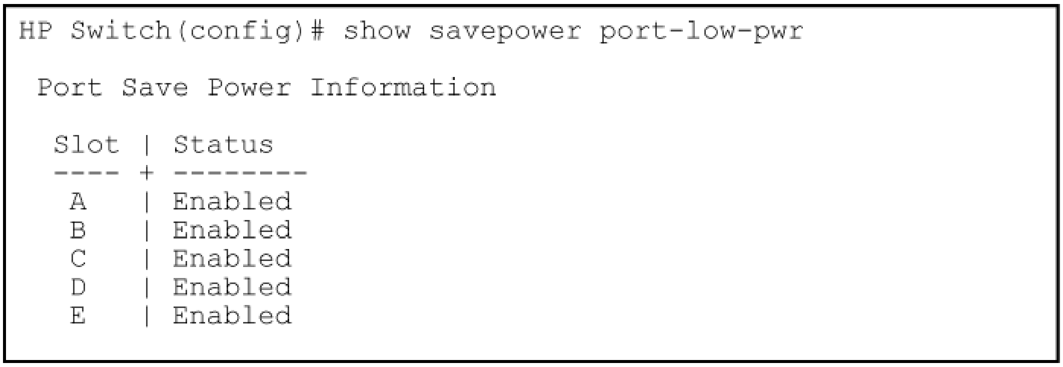
`show savepower` commands

The settings for the `savepower` commands can be viewed using the appropriate `show` command.

show savepower module

Displays the settings for the `savepower module` command (see Figure 266 (page 487)).

Figure 266 Example of output for show savepower module command

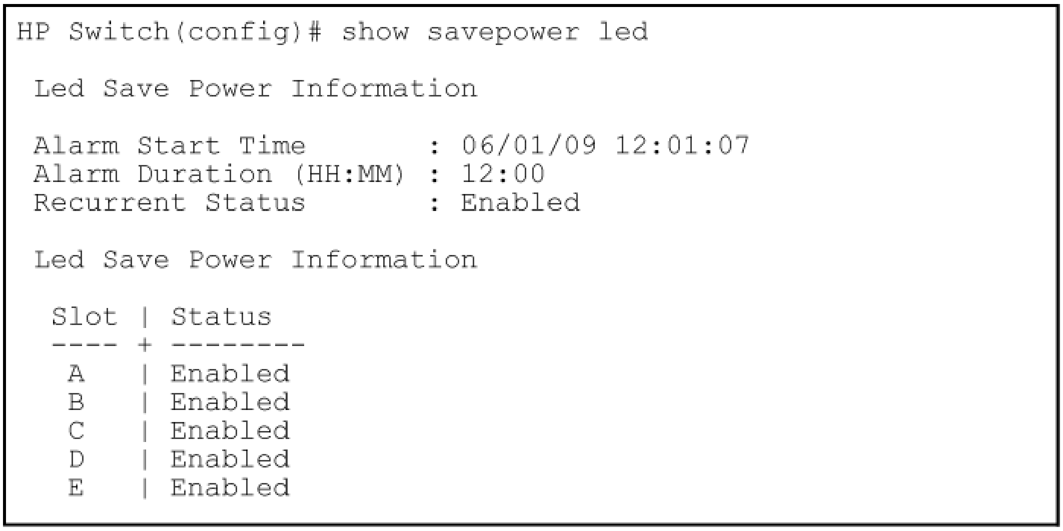


```
HP Switch(config)# show savepower port-low-pwr

 Port Save Power Information

  Slot | Status
  ---- + --------
   A   | Enabled
   B   | Enabled
   C   | Enabled
   D   | Enabled
   E   | Enabled
```

show `savepower port-low-pwr`

Displays the status of the power-down feature for the slots (see Figure 267 (page 488)). For the stackable switches, the output shows if the feature is enabled or not enabled.

Figure 267 Example of output for `show savepower port-low-pwr` command

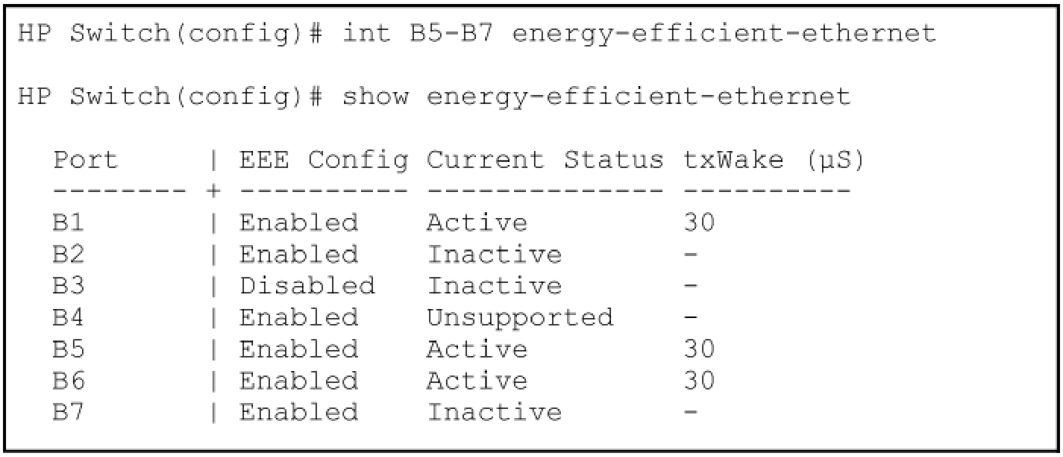


```
HP Switch(config)# show savepower led

 Led Save Power Information

 Alarm Start Time         : 06/01/09 12:01:07
 Alarm Duration (HH:MM)  : 12:00
 Recurrent Status         : Enabled

 Led Save Power Information

  Slot | Status
  ---- + --------
   A   | Enabled
   B   | Enabled
   C   | Enabled
   D   | Enabled
   E   | Enabled
```

show savepower led

Displays the configured status of the LED power-saving option (see Figure 268 (page 488)).

Figure 268 Example of output for `show savepower led` command



```
HP Switch(config)# int B5-B7 energy-efficient-ethernet

HP Switch(config)# show energy-efficient-ethernet

  Port     | EEE Config Current Status txWake (µS)
  -------- + ---------- -------------- ----------
  B1       | Enabled    Active         30
  B2       | Enabled    Inactive       -
  B3       | Disabled   Inactive       -
  B4       | Enabled    Unsupported    -
  B5       | Enabled    Active         30
  B6       | Enabled    Active         30
  B7       | Enabled    Inactive       -
```

Enabling energy efficient ethernet

Energy efficient ethernet (EEE) follows the 802.3az standard, which provides support for a system to operate in low-power idle mode during low-link use. This allows both sides of a link to disable or turn off a portion of the system's transmit/receive circuitry, saving power. When traffic is ready for transmission, the interface sends a "wake-up" message to the link partner to prepare to receive the traffic. The circuitry is returned to "normal" mode. Both sides of the link must be EEE-capable to support the power-saving idle mode.

Syntax:

`[ no ] int` *`port-list`* `energy-efficient-ethernet`

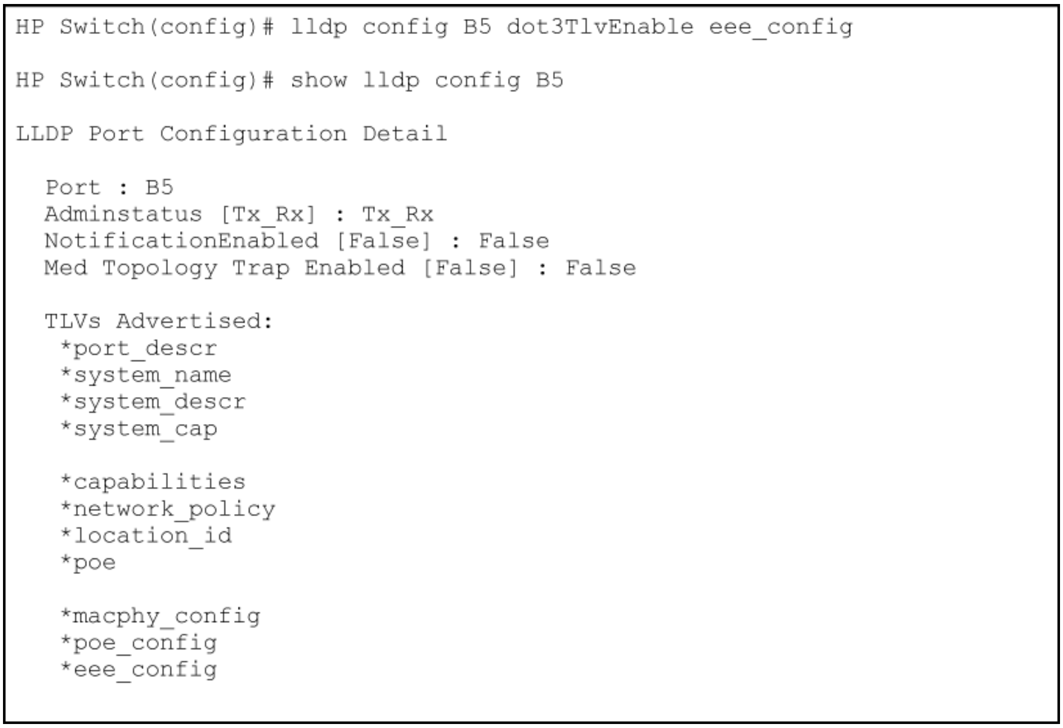
Enables EEE for a given port or range of ports.

The `no` form of the command disables EEE for a port or range of ports.

(Default: Enabled)

Example

Figure 269 EEE enabled on ports B5 - B7



```
HP Switch(config)# lldp config B5 dot3TlvEnable eee_config

HP Switch(config)# show lldp config B5

LLDP Port Configuration Detail

  Port : B5
  Adminstatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False

  TLVs Advertised:
   *port_descr
   *system_name
   *system_descr
   *system_cap

   *capabilities
   *network_policy
   *location_id
   *poe

   *macphy_config
   *poe_config
   *eee_config
```

The parameters are explained in the following table.

Parameter	Description
EEE Config	The EEE configuration status, read from the configuration database.
• Enabled	EEE mode is enabled.
• Disabled	EEE mode is disabled.
Current Status	Current EEE operational status.
• Active	The port is advertised and auto-negotiated EEE with link partner (an EEE-capable partner). EEE mode is enabled.
• Inactive	Set to one of the following conditions: • EEE configuration is disabled on the local port. • Local port advertises EEE capabilities with "EEE disabled" link partner or non-EEE link partner. • Auto-negotiation is mandatory for EEE to work. EEE configuration will not be applied if the port is in forced/manual (speed-duplex) mode. The current status will be 'inactive" for forced/manual mode port configuration. • EEE is not supported for 10Base-T. The current status will be 'inactive' if the link is operating in 10Base-T mode.
• Unsupported	The local physical interface does not have EEE capability.
txWake	Current value of transmit wake-up time (in microseconds).

NOTE: The interface modules do not support adjustment of both transmit and receive wake-up times. Therefore, txWake is constant.

LLDP support for EEE

Layer 2 (data link layer) EEE capability is a feature that allows fine-tuning for EEE that uses LLDP TLVs for the negotiation of physical link partners' wake up time values. An EEE-capable port notifies its link partner about the EEE capabilities supported. The ports then negotiate how to best optimize energy efficiency.

Syntax:

```
[ no ] lldp config port-list dot3TlvEnable eee_config
```

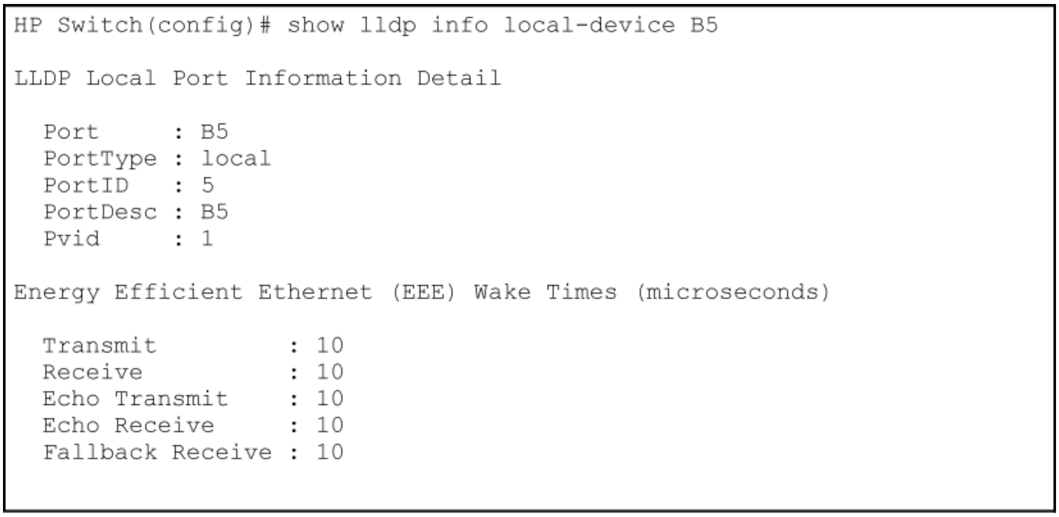
Enables the advertisement of Layer 2 EEE TLVs for a given port or range of ports.

The no form of the command disables the advertisement of EEE TLVs.

(Default: Enabled)

Examples

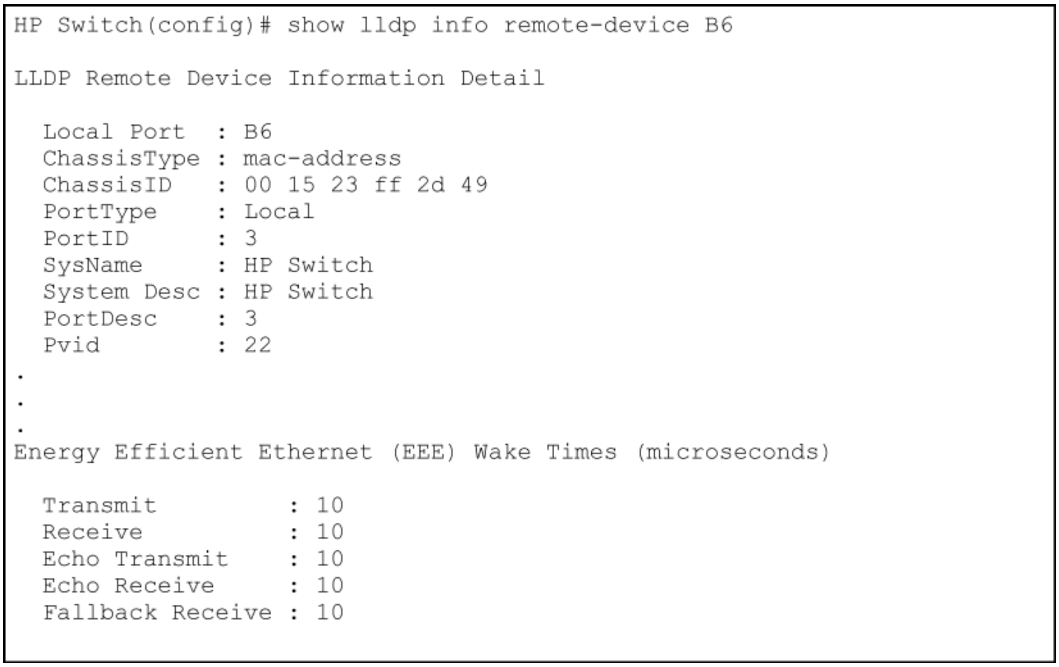
Figure 270 Configuring Layer 2 TLVs on a port



```
HP Switch(config)# show lldp info local-device B5

LLDP Local Port Information Detail

  Port     : B5
  PortType : local
  PortID   : 5
  PortDesc : B5
  Pvid     : 1

Energy Efficient Ethernet (EEE) Wake Times (microseconds)

  Transmit          : 10
  Receive           : 10
  Echo Transmit     : 10
  Echo Receive      : 10
  Fallback Receive : 10
```

To display the EEE TLV information for the local port, enter the `show lldp info local-device` *`port-list`* command, as shown in Figure 271 (page 491).

Figure 271 Output for LLDP information for a local port



```
HP Switch(config)# show lldp info remote-device B6

LLDP Remote Device Information Detail

  Local Port  : B6
  ChassisType : mac-address
  ChassisID   : 00 15 23 ff 2d 49
  PortType    : Local
  PortID      : 3
  SysName     : HP Switch
  System Desc : HP Switch
  PortDesc    : 3
  Pvid        : 22
.
.
.
Energy Efficient Ethernet (EEE) Wake Times (microseconds)

  Transmit          : 10
  Receive           : 10
  Echo Transmit     : 10
  Echo Receive      : 10
  Fallback Receive : 10
```

To display the EEE TLV information for the link partner, enter the `show lldp info remote-device` *`port-list`* command, as shown in Figure 33 (page 89).

J Network Out-of-Band Management (OOBM) for the 6600 Switch

Command summary

Table 46 Summary of commands

Command syntax	Description	Default	CLI reference	Menu reference
`oobm`	Enters the OOBM context from the general configuration context.		(page 494)	
`enable` `disable`	Enables or disables networked OOBM on the switch from the OOBM context.	Enabled	(page 494)	

`oobm enable`
`oobm disable`
	Enables or disables networked OOBM on the switch from the general configuration context.	Enabled	(page 494)	

`interface [ enable | disable ]`	Enables or disables the networked OOBM interface (port) from the OOBM context.		(page 494)	
`oobm interface [ enable | disable ]`	Enables or disables the networked OOBM interface (port) from the general configuration context.		(page 494)	
`interface speed-duplex [ 10-half | 10-full | 100-half | 100-full | auto ]`	Enables or disables the networked OOBM interface (port) from the OOBM context.		(page 495)	
`oobm interface speed-duplex [ 10-half | 10-full | 100-half | 100-full | auto ]`	Enables or disables the networked OOBM interface (port)from the general configuration context.		(page 495)	
`[no] ip address [ dhcp-bootp | ip-address/mask-length ]`	Configures an IPv4 address for the switch's OOBM interface from the OOBM context.		(page 495)	
`[no] oobm ip address [ dhcp-bootp | ip-address/mask-length ]`	Configures an IPv4 address for the switch's OOBM interface from the general configuration context.		(page 495)	
`[no] ip default-gateway` *`ip-address`*	Configures an IPv4 default gateway for the switch's OOBM interface from the OOBM context.		(page 496)	
`[no] oobm ip default-gateway` *`ip-address`*	Configures an IPv4 default gateway for the switch's OOBM interface from the general configuration context.		(page 496)	
`show oobm`	Summarizes OOBM configuration information.		(page 496)	
`show oobm ip`	Summarizes the IP configuration of the OOBM interface.		(page 496)	
`show oobm arp`	Summarizes the ARP table entries for the OOBM interface.		(page 497)	

Table 46 Summary of commands *(continued)*

Command syntax	Description	Default	CLI reference	Menu reference
`interface` `-server [listen oobm | data | both ]`	Application servers have added a `listen` keyword with `oobm|data|both` options to specify which interfaces are active.	Both	(page 497)	

Telnet:
`telnet ip-address [oobm]`
TFTP:
`copy tftp ... ip-address filename... [oobm]`
SNTP:
`[ no ] sntp server priority priority ip-address [oobm] [version]`
TIMEP:
`[no] ip timep dhcp | manual ip-address | [oobm] [...]`
RADIUS:
`[ no ] radius-server host ip-address [oobm]`
TACACS+:
`[ no ] tacacs-server host ip-address [oobm]`
DNS:
`[ no ] ip dns server-address priority priority ip-address [oobm]`
Syslog:
`[ no ] logging ip-address [[control-descr] | [oobm]]`
Ping:
`ping [ ...] [source [ ip-address | vlan-id | oobm ]]`
Traceroute:
`traceroute [...] [source ip-address | vlan-id | oobm ]`
	CLI commands for client applications have added the `oobm` keyword to allow you to specify that the outgoing request be issued from the OOBM interface.		(page 498)	

For conceptual information about the following commands, see “Concepts” (page 500).

OOBM Configuration

OOBM configuration commands can be issued from the global configuration context (config) or from a specific OOBM configuration context (oobm).

Entering the OOBM configuration context from the general configuration context

Syntax:

```
oobm
```

Enters the OOBM context from the general configuration context.

Example

```
HP Switch (config)# oobm
HP Switch (oobm)#
```

Enabling and disabling OOBM

From the OOBM context:

Syntax:

```
enable
disable
```

From the general configuration context:

Syntax:

```
oobm enable
oobm disable
```

Enables or disables networked OOBM on the switch.

OOBM is not compatible with either a management VLAN or stacking. If you attempt to enable OOBM when a management VLAN is enabled or when stacking is enabled, the command will be rejected and you will receive an error message.

If an OOBM IP address exists and you disable OOBM, the OOBM IP address configuration is maintained. If you enable OOBM and there is a pre-existing OOBM IP address, it will be reinstated.

Network OOBM is enabled by default.

Examples

```
HP Switch (oobm)# enable
HP Switch (oobm)# disable
HP Switch (config)# oobm enable
HP Switch (config)# oobm disable
```

Enabling and disabling the OOBM port

The OOBM `interface` command enables or disables the OOBM interface (that is, the OOBM port, as opposed to the OOBM function).

From the OOBM context:

Syntax:

```
interface [ enable | disable ]
```

From the general configuration context:

Syntax:

```
oobm interface [ enable | disable ]
```

Enables or disables the networked OOBM interface (port).

Examples

```
HP Switch (oobm)# interface enable
HP Switch (config)# oobm interface disable
```

Setting the OOBM port speed

The OOBM port operates at 10 Mbps or 100 Mbps, half or full duplex. These can be set explicitly or they can be automatically negotiated using the `auto` setting.

From the OOBM context:

Syntax:

```
interface speed-duplex [ 10-half | 10-full | 100-half |
100-full | auto ]
```

From the general configuration context:

Syntax:

```
oobm interface speed-duplex [ 10-half | 10-full | 100-half |
100-full | auto ]
```

Enables or disables the networked OOBM interface (port). Available settings are:

`10-half`	10 Mbps, half-duplex
`10-full`	10-Mbps, full-duplex
`100-half`	100-Mbps, half-duplex
`100-full`	100-Mbps, full-duplex
`auto`	auto negotiate for speed and duplex

Example

```
HP Switch (oobm)# interface speed-duplex auto
```

Configuring an OOBM IPv4 address

Configuring an IPv4 address for the OOBM interface is similar to VLAN IP address configuration, but it is accomplished within the OOBM context.

From the OOBM context:

Syntax:

```
[ no ] ip address [ dhcp-bootp | ip-address/mask-length ]
```

From the general configuration context:

Syntax:

```
[ no ] oobm ip address [ dhcp-bootp | ip-address/mask-length
]
```

Configures an IPv4 address for the switch's OOBM interface.

You can configure an IPv4 address even when global OOBM is disabled; that address will become effective when OOBM is enabled.

Example

```
HP Switch (oobm)# ip address 10.1.1.17/24
```

Configuring an OOBM IPv4 default gateway

Configuring an IPv4 default gateway for the OOBM interface is similar to VLAN default gateway configuration, but it is accomplished within the OOBM context.

From the OOBM context:

Syntax:

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

From the general configuration context:

Syntax:

```
[ no ] oobm ip default-gateway ip-address
```

Configures an IPv4 default gateway for the switch's OOBM interface.

Example

```
HP Switch (oobm)# ip default-gateway 10.1.1.1
```

OOBM show commands

The `show` commands for OOBM are similar to the analogous commands for the data plane. Note that you must always include the `oobm` parameter to see the information for the OOBM interface, regardless of the context. For instance, even from the OOBM context, the `show ip` command displays the IP configuration for the data plane; to see the IP configuration of the OOBM interface, you need to use `show oobm ip`.

Showing the global OOBM and OOBM port configuration

Syntax:

```
show oobm
```

Summarizes OOBM configuration information. This command displays the global OOBM configuration (enabled or disabled), the OOBM interface status (up or down), and the port status (enabled/disabled, duplex, and speed).

You can issue this command from any context

Example

```
HP Switch# show oobm

Global Configuration
  OOBM Enabled   : Yes
  OOBM Port Type  : 10/100TX
  OOBM Interface Status : Up
  OOBM Port    : Enabled
  OOBM Port Speed  : Auto
```

Showing OOBM IP configuration

Syntax:

```
show oobm ip
```

Summarizes the IP configuration of the OOBM interface. This command displays the status of IPv4 (enabled/disabled), the IPv4 default gateway, and the IPv4 address configured for the interface.

You can issue this command from any context.

Example

```
HP Switch# show oobm ip
```

Showing OOBM ARP information

Syntax:

```
show oobm arp
```

Summarizes the ARP table entries for the OOBM interface.

You can issue this command from any context.

Example

HP Switch# show oobm arp

Application server commands

Application servers (as described in OOBM and server applications in "Concepts" (page 500)) have added a `listen` keyword with `oobm|data|both` options to specify which interfaces are active.

Default value is `both` for all servers.

Telnet:
`telnet-server [listen  oobm | data | both  ]`
Management and Configuration Guide

SSH:
`ip ssh [listen  oobm | data | both  ]`
Access Security Guide

SNMP:
`snmp-server [listen  oobm | data | both  ]`
Management and Configuration Guide

TFTP:
`tftp server [listen  oobm | data | both  ]`
Management and Configuration Guide

HTTP:
`web-management [listen  oobm | data | both  ]`
Management and Configuration Guide

In all cases, `show running-config` displays the server configurations.

Use the no form of the command to prevent the server from running on either interface.

Examples

Telnet: `no telnet-server`

SSH: `no ip ssh` …

SNMP: `no snmp-server` …

TFTP: `no tftp server`

HTTP: `no web-management` …

The `show servers` command shows the listen mode of the servers:

```
HP Switch# show servers
Server listen mode

Server   Listen mode
-----------------------------
Telnet        | both
Ssh         | both
Tftp        | both
Web-management | both
Snmp        | both
```

Application client commands

CLI commands for client applications have added the `oobm` keyword to allow you to specify that the outgoing request be issued from the OOBM interface. If you do not specify the `oobm` keyword, the request will be issued from the appropriate in-band data interface. Command syntax is:

Telnet:

```
telnet ip-address [oobm]
```

Management and Configuration Guide

TFTP:

```
copy tftp ... ip-address filename... [oobm]
```

Management and Configuration Guide

SNTP:

```
[ no ] sntp server priority priority ip-address [oobm] [version]
```

Management and Configuration Guide

TIMEP:

```
[ no ] ip timep [ dhcp | manual ip-address | [oobm]] [...]
```

Management and Configuration Guide

RADIUS:

```
[ no ] radius-server host ip-address [oobm]
```

Access Security Guide

TACACS+:

```
[ no ] tacacs-server host ip-address [oobm]
```

Access Security Guide

DNS:

```
[ no ] ip dns server-address priority priority ip-address [oobm]
```

Management and Configuration Guide

Syslog:

```
[ no ] logging ip-address [[control-descr] | [oobm]]
```

Management and Configuration Guide

Ping:

```
ping [ ...] [source [ ip-address | vlan-id | oobm ]]
```

Management and Configuration Guide

Traceroute:

```
traceroute [...] [source [ ip-address | vlan-id | oobm ]]
```

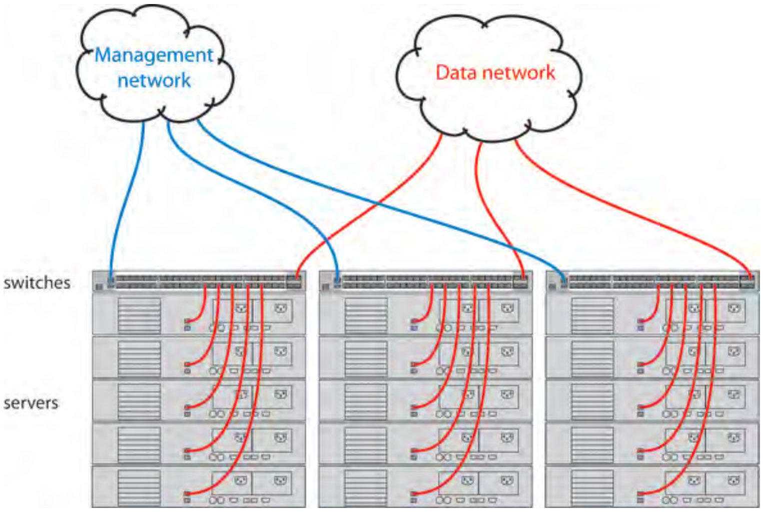
Management and Configuration Guide

Example

Figure 272 (page 499) shows setup and use of network OOBM using the commands described above.

Assume that the figure below describes how you want to set up your data center.

Figure 272 Example data center



Assume that you are configuring the switch in the left-hand rack to communicate on both the data and management networks. You might do the following:

- Configure an IP address on the data network.
- Verify that out-of-band management is enabled. (It is enabled by default.)
- Configure an IP address on the management network.
- Verify that the switch can communicate on both networks.

The CLI commands that follow would accomplish those tasks. (The first time through the process you might easily make the omission shown near the end of the example.)

```
Switch 41# config
Switch 41(config)# vlan 1
Switch 41(vlan-1)# ip address 10.1.129.7/20        Set up IP address on data network.
Switch 41(vlan-1)# end                                  Exit back to manager context.
Switch 41# show oobm                              Look at default OOBM configuration.

Global Configuration
  OOBM Enabled   : Yes
  OOBM Port Type  : 10/100TX
  OOBM Interface Status : Up                            Defaults look appropriate.
  OOBM Port   : Enabled
  OOBM Port Speed  : Auto

Switch 41# config
Switch 41(config)# oobm                                    Go to OOBM context and
Switch 41(oobm)# ip address 10.255.255.41/24                   add IP address and
Switch 41(oobm)# ip default-gateway 10.255.255.1                  default gateway.
Switch 41(oobm)# end                                    Exit back to manager context.
Switch 41# ping 10.1.131.44             Ping server in this rack (on data network).
10.1.131.44 is alive, time = 19 ms
Switch 41# ping 10.1.131.51                             Ping server in adjacent rack.
10.1.131.51 is alive, time = 15 ms
Switch 41# ping 10.255.255.42                           Ping switch in adjacent rack.
The destination address is unreachable.       Oops! It’s on the management network.
Switch 41# ping source oobm 10.255.255.42           Go through the management port
10.255.255.42 is alive, time = 2 ms                              and it works fine.
Switch 41#
```

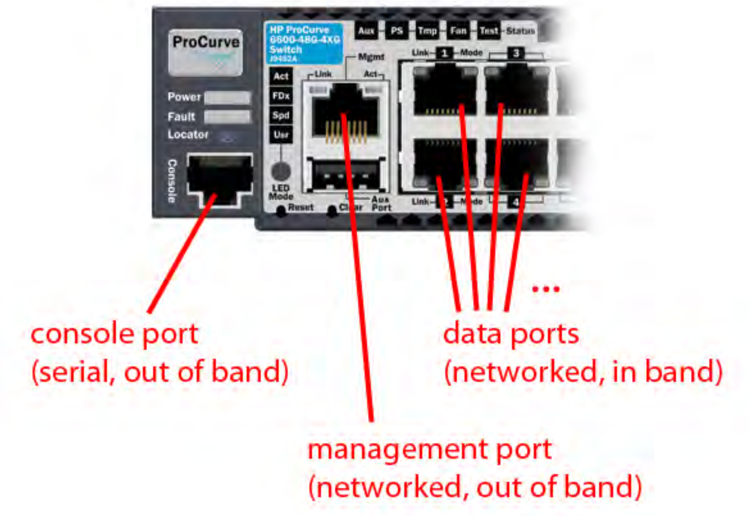
Concepts

Management communications with a managed switch can be:

- In band—through the networked data ports of the switch
- Out of band—through a dedicated management port (or ports) separate from the data ports

Out-of-band ports have typically been serial console ports using DB-9 or specially wired 8-pin modular (RJ-style) connectors. Some recent HP switches have added networked OOBM ports. Figure 273 (page 500) shows management connections for a typical switch.

Figure 273 Management ports



OOBM operates on a "management plane" that is separate from the "data plane" used by data traffic on the switch and by in-band management traffic. That separation means that OOBM can continue to function even during periods of traffic congestion, equipment malfunction, or attacks on the network. In addition, it can provide improved switch security: a properly configured switch can limit management access to the management port only, preventing malicious attempts to gain access via the data ports.

Network OOBM typically occurs on a management network that connects multiple switches. It has the added advantage that it can be done from a central location and does not require an individual physical cable from the management station to each switch's console port.

Of the switches covered by this manual, network OOBM is available on:

- HP Switch 6600-24XG switch (J9265A)
- HP Switch 6600-48G switch (J9451A)
- HP Switch 6600-48G-4XG switch (J9452A)

Table 47 (page 500) summarizes the switch management ports.

Table 47 Switch management ports

	In band	Out of band	
	Networked	**Directly connected**	**Networked**
Management interface	Command line (CLI), menu, Web	Command line (CLI), menu	Command line (CLI), menu
Communication plane	Data plane	Management plane	Management plane
Connection port	Any data port	Dedicated serial or USB console port	Dedicated networked management port

Table 47 Switch management ports *(continued)*

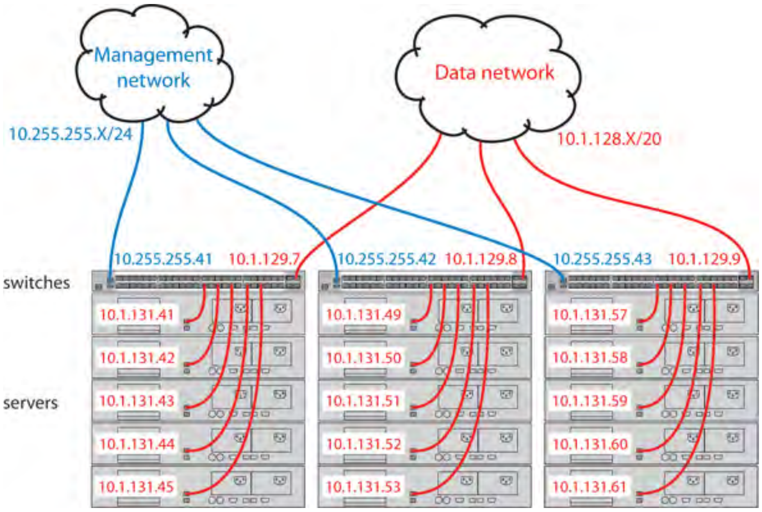
	In band	Out of band	
	Networked	**Directly connected**	**Networked**
Connector type	Usually RJ-45; also CX4, SFP, SFP+, and XFP	DB9 serial, serial-wired 8-pin RJ	RJ-45
Advantages	Allows centralized management	Not affected by events on data network, shows boot sequence	Not affected by events on data network, allows centralized management, allows improved security
Disadvantages	Can be affected by events on data network; does not show boot sequence	Requires direct connection to console port (can be done via networked terminal server)	Does not show boot sequence

Example

In a typical data center installation, top-of-rack switches connect servers to the data network, while the management ports of those switches connect to a physically and logically separate management network. This allows network administrators to manage the switches even if operation on the data network is disrupted.

In Figure 274 (page 501), the switches face the hot aisle of the data center, allowing easy connection to the network ports on the backs of the servers.

Figure 274 Network OOBM in a data center



For even more control, the serial console ports of the switches can be connected to the management network through a serial console server (essentially, a networked serial switch), allowing the network administrators to view the CLI activity of each switch at boot time and to control the switches through the console ports (as well as through the management ports).

OOBM and switch applications

The table below shows the switch applications that are supported on the OOBM interface as well as on the data interfaces. In this list, some applications are client-only, some are server-only, and some are both.

Application	Inbound OOBM (server)	Outbound OOBM (client)	Inbound data plane (server)	Outbound data plane (client)
Telnet	yes	yes	yes	yes
SSH	yes	[1]	yes	[1]
SNMP	yes	yes[2]	yes	yes
TFTP	yes	yes	yes	yes
HTTP	yes	[1]	yes	[1]
SNTP	[1]	yes	[1]	yes
TIMEP	[1]	yes	[1]	yes
RADIUS	[1]	yes	[1]	yes
TACACS	[1]	yes	[1]	yes
DNS[3]	[1]	yes	[1]	yes
Syslog	[1]	yes	[1]	yes
Ping	yes[4]	yes	yes[4]	yes
Traceroute	yes[4]	yes	yes[4]	yes

[1] N/A = not applicable

[2] *=SNMP client refers to SNMP traps as they originate from the switch.

[3] **=DNS has a limit of two servers—primary and secondary. Either can be configured to use the OOBM interface.

[4] ***=Ping and Traceroute do not have explicit servers. Ping and Traceroute responses are sent by the host stack.

For applications that have servers, `oobm/data/both` options have been added to listen mode. There is now a `listen` keyword in the CLI commands to allow selection of those options. Default **value** is `both` for all servers. For details of the new command syntax, see Support and Other Resources (page 503).

K Support and Other Resources

Intended audience

This guide is intended for network administrators with intermediate-to-advanced knowledge of computer networking.

Related documentation

The following sources provide related information:

- *Power over Ethernet (PoE/PoE+) Planning and Implementation Guide*
- *HP Switch 620 Redundant and External Power Suppy Installation and Getting Started Guide*
- *HP Switch 630 Redundant and/or External Power Supply Installation and Getting Started Guide*
- *HP Management and Configuration Guide*
- *HP Advanced Traffic Management Guide*
- *HP Access Security Guide*
- *HP Multicast and Routing Guide*
- *HP IPv6 Configuration Guide*

You can also find the documents referenced in this guide on the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals.

Contacting HP

HP technical support

For worldwide technical support information, see the HP support website:

http://www.hp.com/networking/support.

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's choice for business website:

http://www.hp.com/go/e-updates

After registering, you will receive email notifications of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

HP websites

- HP:
  http://www.hp.com
- HP Networking:
  http://www/hp.com/go/networking
- HP Partner Locator:
  http://www.hp.com/service_locator
- HP Software Downloads:
  http://www.hp.com/support/downloads

Typographical conventions

Table 48 Document conventions

Convention	Element
Blue text: Table 26	Cross-reference links and email addresses
Blue underlined text: http://www.hp.com	Website addresses
Bold text	• Keys that are pressed • Text entered into a GUI element, such as a box • Text entered as a CLI command • GUI elements that are clicked or selected, such as menu and list items, buttons, tabs, and check boxes
Italic text	• Text emphasis • Variables for which you must supply a value when executing a command
`Monospace` text	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace italic` text	• Code variables • Command variables
`Monospace bold` text	Emphasized monospace text
. . .	Indication that example continues

Command syntax statements

Syntax

```
ip  default-gateway ip-addr  | routing
```

Syntax

```
show interfaces [port-list]
```

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ( ) enclose required elements.
- Braces within square brackets ([ ]) indicate a required element within an optional choice.
- Boldface indicates use of a CLI command, part of a CLI command syntax, or other displayed element in general text. For example:

"Use the `copy tftp` command to download the key from a TFTP server."

- Italics indicate variables for which you must supply a value when executing the command. For example, in this command syntax, you must provide one or more port numbers:

aaa port-access authenticator *port-list*

Command prompts

In the default configuration, your switch displays a CLI prompt similar to the following example:

```
HP Switch 8212zl#
```

To simplify recognition, this guide uses `HP Switch` to represent command prompts for all switch models. For example:

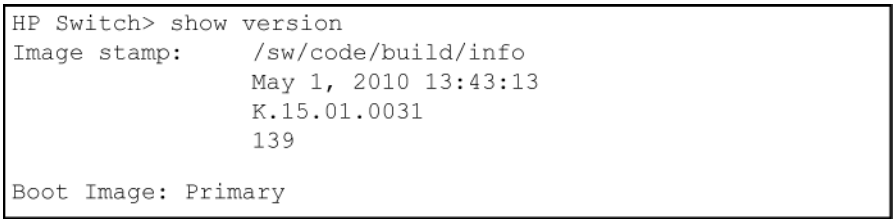
```
HP Switch#
```

(You can use the `hostname` command to change the text in the CLI prompt.)

Screen simulations

Figures containing simulated screen text and command output look similar to this:

Figure 275 Example of a simulated screen



```
HP Switch> show version
Image stamp:     /sw/code/build/info
                 May 1, 2010 13:43:13
                 K.15.01.0031
                 139

Boot Image: Primary
```

In some cases, brief command-output sequences appear without figure identification. For example:

```
HP Switch(config)# clear public-key
HP Switch(config)# show ip client-public-key
show_client_public_key: cannot stat keyfile
```

Configuration and operation examples

Unless otherwise noted, examples using a particular switch model apply to all switch models covered by this guide.

Keys

Simulations of actual keys use a bold, sans-serif typeface with square brackets. For example, the Tab key appears as **[Tab]** and the "Y" key appears as **[Y]**.

To set up and install the switch in your network

Physical installation

Use the *Installation and Getting Started Guide* for the following:

- Notes, cautions, and warnings related to installing and using the switch and its related modules.
- Instructions for physically installing the switch in your network.
- Quickly assigning an IP address and subnet mask, setting a Manager password, and (optionally) configuring other basic features.
- Interpreting LED behavior.

For the latest version of the *Installation and Getting Started Guide* for your switch, see "Getting documentation from the web".

Product warranties

For information about HP Networking product warranties, see the warranty information website:

http://www.hp.com/networking/support

Table 49 (page 506) lists related products and their part numbers.

Table 49 Applicable Products

Product	Part Number
HP Switch E3500yl-24G-PoE+ Switch	J9310A
HP Switch E3500yl-48G-PoE+ Switch	J9311A
HP Switch 10GbE 2-Port SFP+/2-Port CX4 yl Module	J9312A
630 Redundant and/or External Power Supply	J9443A
E3500-24 Switch	J9470A
E3500-48 Switch	J9472A
E3500-24-PoE Switch	J9471A
E3500-48-PoE Switch	J9473A
E3500yl-24G-PWR Intelligent Edge	J8692A
E3500yl-48G-PWR Intelligent Edge	J8693A
Switch E6200yl-24G mGBIC Premium Edge	J8992A
Switch E3500yl 2p 10GbE X2 + 2p CX4 Module	J8694A
620 Redundant and External Power Supply	J8696A
Switch E3500yl/E6200yl Fan Tray	5069-8598
Switch E3500yl/E6200yl Rack Mounting Kit	5069-5705
Switch E3500yl/E6200yl 10K Rack Rail Kit	356578-B21
Switch zl and yl RPS/EPS Cable	5070-0102

Online help

Menu interface

If you need information on specific parameters in the menu interface, refer to the online help provided in the interface.

Command-line interface

If you need information on a specific command in the CLI, type the command name followed by the word `help`.

HP customer support services

If you are having trouble with your switch, Hewlett-Packard offers support 24 hours a day, seven days a week through the use of a number of automated electronic services. See the Customer Support/Warranty booklet that came with your switch for information on how to use these services to get technical support. HP provides up-to-date customer care, support, and warranty information at

www.hp.com/networking/support.

Your HP authorized network reseller can also provide assistance, both with services that they offer and with services offered by HP.

Before calling support

Before calling your networking dealer or HP Support, to make the support process most efficient, first retrieve the following information:

Information item	Information location
Product identification, including mini-GBICs	The front of the switch and on labels on the mini-GBICs
Details about the switch—status including the software (OS) version, a copy of the switch configuration, a copy of the switch Event Log, and a copy of the switch status and counters information	Switch console: `show tech` command
Copy of your network topology map, including network addresses assigned to the relevant devices	Your network records

Glossary of terms and acronyms

ACE Access control entry

ACL Access control list

active PoE port A PoE-enabled port connected to a PD requesting power.

active port A port linked to another active device (regardless of whether MSTP is blocking the link).

adjacent device See "Neighbor or Neighbor Device"

advertisement See LLDPDU

all-traffic rate-limiting Applies a rate-limit to all traffic (including ICMP traffic) on an interface.

AM Active management module. A management module that booted successfully and is actively managing the switch.

bps bits per second

BSD rcp Berkeley UNIX remote copy

CDP Cisco discovery protocol. Supports reading CDP packets received from neighbor devices, enabling a switch to learn about adjacent CDP devices.

chassis Hardware operation, including modules and ports, power supply, fans, transceivers, CPU interrupt errors, switch temperature, and so on.

classifier-based mirroring policy The service policy applied to a monitored (port or VLAN) interface that specifies the classes of traffic to be copied to preconfigured mirroring destinations.

CoS Class of service. Provides priority handling of packets traversing the switch, based on the IEEE 802.1p priority carried by each packet.

DCA Dynamic configuration arbiter. Determines the client-specific parameters that are assigned in an authentication session.

destination The host device that is connected to an exit port on the local source switch or a remote switch, and associated with a mirrorsession number (1 to 4). See also Exit Port and Host.

DHCP Dynamic host configuration protocol

direction-based mirroring On an interface configured for mirroring, the traffic direction (entering or leaving the switch, or both) is used as criteria for selecting the traffic to be mirrored.

DLC data link layer classification

DLL data link layer

DMA Direct access memory. Transmits and receives packets between the CPU and the switch.

DNS Domain name system

domain suffix Includes all labels to the right of the unique host name in a fully qualified domain name assigned to an IP address. For example, in the fully qualified domain name "device53.evergreen.trees.org," the domain suffix is "evergreen.trees.org," while "device53" is the unique (host) name assigned to a specific IP address.

DoS Denial of service

DT Distributed trunk

DTD Distributed trunking device

DTE Data terminal equipment

DTIP Distributed trunking internet protocol

DTS Distributed trunking switches

ECS Emergency call service

EEE Energy efficient ethernet

ELIN Emergency location identification number. A valid telephone number in the North American Numbering Plan format and assigned to a multiline telephone system operator by the appropriate authority. This number calls a public service answering point (PSAP) and relays automatic location identification data to the PSAP.

exit port The port to which a traffic analyzer or IDS is connected to receive mirrored traffic.

- For local mirroring, an exit port can be any port to which a traffic analyzer or IDS is connected and that is not configured as a monitored interface. You can configure up to four exit ports for local mirroring on a switch, using the command: `mirror session port exit-port`
- For remote mirroring, the destination IP address (dst-ip) and exit port in a remote mirroring endpoint can belong to different VLANs. You can configure up to 32 exit ports for remote mirroring on a switch, using the command: mirror `endpoint ip src-ip src-udp-port dst-ip exit-port`

CAUTION: An exit port should be connected only to a network analyzer, IDS, or other network edge device that has no connection to other network resources. Connecting a mirroring exit port to a network can result in serious network performance problems, and is strongly discouraged by HP Switches Networking.

exit switch The switch with the exit port to which a destination device is connected. See also Exit Port.

failed management module A management module that did not pass selftest and is not in standby mode.

FFI (event type) Find, fix, and inform. Event or alert log messages indicating a possible topology loop that causes excessive network activity and results in the network running slow.

FIB Forwarding information base.

fixed or "well-known" traps A switch automatically sends fixed traps (such as "coldStart", "warmStart", "linkDown", and "linkUp") to trap receivers using the public community name. These traps cannot be redirected to other communities. If you change or delete the default public community name, these traps are not sent.

fully qualified domain name The sequence of labels in a domain name identifying a specific host (host name) and the domain in which it exists. For example, if a device with an IP address of 10.10.10.101 has a host name of device53 and resides in the evergreen.trees.org domain, the device's fully qualified domain name is device53.evergreen.trees.org and the DNS resolution of this name is 10.10.10.101.

GARP Generic attribute registration protocol (defined in the IEEE 802.1D-1998 standard).

GMB Guaranteed minimum bandwidth. Provides a method for ensuring that each of a given port's outbound traffic priority queues has a specified minimum consideration for sending traffic out on the link to another device. This can prevent a condition where applications generating lower-priority traffic in the network are frequently or continually "starved" by high volumes of higher-priority traffic.

GVRP GARP VLAN registration protocol. Manages dynamic 802.1Q VLAN operations, in which the switch creates temporary VLAN membership on a port to provide a link to another port in the same VLAN on another device.

host Used in traffic mirroring to refer to a traffic analyzer or IDS.

host name The unique, leftmost label in a domain name assigned to a specific IP address in a DNS server configuration. This enables the server to distinguish a device using that IP address from other devices in the same domain. For example, in the evergreen.trees.org domain, if an IPv4 address of 10.10.100.27 is assigned a host name of accounts015 and another IP address of 10.10.100.33 is assigned a host name of sales021, the switch configured with the domain suffix evergreen.trees.org and a DNS server that resolves addresses in that domain can use the host names to reach the devices with DNS-compatible commands.

For example: `ping accounts015` `traceroute accounts015`

ICMP Internet control message protocol.

ICMP Rate-Limiting Applies a rate-limit to all inbound ICMP traffic received on an interface, but does not limit other types of inbound traffic.

IDM Identify-driven management.

IDS Intrusion detection system.

IGMP Internet group management protocol.

IP addressing Internet protocol (addressing)Configures the switch with an IP address and subnet mask to communicate on the network and support remote management access; configures multiple IP addresses on a VLAN; enables IP routing on the switch.

ISC InterSwitch connect. A special interface that connects DTSs.

jumbo frame An IP frame exceeding 1522 bytes in size. The maximum Jumbo frame size is 9220 bytes. (This size includes 4 bytes for the VLAN tag.)

jumbo VLAN A VLAN configured to allow inbound jumbo traffic. All ports belonging to a jumbo and operating at 1 Gbps or higher can receive jumbo frames from external devices. If the switch is in a meshed domain, then all meshed ports (operating at 1 Gbps or higher) on the switch will accept jumbo traffic from other devices in the mesh.

KMS Key management system.

LACP Link aggregation control protocol.

link test A test of the connection between the switch and a designated network device on the same LAN (or VLAN, if configured).

LLDP Link layer discovery protocol. Provides a standards-based method for enabling the switches covered in this guide to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

LLDP neighbor An LLDP device that is either directly connected to another LLDP device or connected to that device by another, non- LLDP Layer 2 device (such as a hub) Note that an 802.1D-compliant switch does not forward LLDP data packets even if it is not LLDP-aware.

LLDP-aware A device that has LLDP in its operating code, regardless of whether LLDP is enabled or disabled.

LLDP-MED LLDP-media-endpoint-discovery. LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP (IEEE 802.1AB) industry standard to support advanced features on the network edge for Voice Over IP (VoIP) endpoint devices with specialized capabilities and LLDP-MED standardsbased functionality.

LLDP-MED Second description for this acronym. The TIA telecommunications standard produced by engineering subcommittee TR41.4, "VoIP Systems - IP Telephony infrastructure and Endpoints" to address needs related to deploying VoIP equipment in IEEE 802-based environments. This standard will be published as ANSI/TIA- 1057.

LLDPDU LLDP data unit. LLDP data unitLLDP data packet are transmitted on active links and include multiple TLVs containing global and perport switch information. In this guide, LLDPDUs are termed "advertisements" or "packets".

local mirroring The monitored (source) interface and exit port in a mirroring session are on the same switch.

local mirroring traffic destination Port on the same switch as the source of the traffic being mirrored. See also remote mirroring traffic destination.

log throttle periods Used to regulate (throttle) duplicate messages for recurring events.

LSA Link-state advertisements.

MED Media endpoint discovery/devices (see LLDPMED).

MIB Management information base. An internal database the switch maintains for configuration and performance information.

MLD Multicast listener discovery. IPv6 protocol used by a router to discover the presence of multicast listeners. MLD can also optimize IPv6 multicast traffic flow with the snooping feature.

MLTS Multiline telephone system/service. A network-based and/or premises-based telephone system having a common interface with the public switched telephone system and having multiple telephone lines, common control units, multiple telephone sets, and control hardware and software.

mm Management module.

monitored interface The interface (port, VLAN, trunk, or mesh) on the source switch on which the inbound and/or outbound traffic to be mirrored originates , configured with one of the interface monitor or vlan monitor commands.

MPS Maintenance power signature. The signal a PD sends to the switch to indicate that the PD is connected and requires power.

MSTP Multiple spanning tree protocol.

MTM Multicast traffic manager. Controls and coordinates L3 multicast traffic for upper layer protocols.

MTU Maximum transmission unit. The maximum size IP frame the switch can receive for Layer 2 frames inbound on a port.

NANP North American numbering plan. A ten-digit telephone number format where the first three digits are an area code and the last seven-digits are a local telephone number.

Neighbor See LLDP Neighbor.

non-LLDP device A device that is not capable of LLDP operation.

nonstop switching The standby management module is synced continuously with the active management module so that all features and config files are the same on both management modules. The standby management module is ready to become the active management module. The transition is quick and seamless; switching continues without interruption.

offline management module A management module that is offline because Management Module redundancy is disabled.

OOBM out-of-band management

OSPF Open short path first. A routing protocol that uses link-state advertisements (LSA) to update neighboring routers regarding its interfaces and information on those interfaces. Each routing switch maintains an identical database that describes its area topology to help a router determine the shortest path between it and any neighboring router.

oversubscribed The state where there are more PDs requesting PoE power than can be accommodated.

oversubscribed queue The condition where there is insufficient bandwidth allocated to a particular outbound priority queue for a given port. If additional, unused bandwidth is not available, the port delays or drops the excess traffic.

PCM HP Switch Manager. Windows-based network management solutions for managing and monitoring performance of HP devices.

PCM (+) HP Switch Manager Plus. See PCM.

PD Powered device. An IEEE 802.3af-compliant or IEEE 802.3at-compliant device that receives its power through a direct connection to a 10/ 100Base-TX PoE RJ-45 port in an HP fixed-port or chassis-based switch. Examples of PDs include Voice-over-IP (VoIP) telephones, wireless access points, and remote video cameras.

PIM Protocol-independent multicast (routing). Enables IP multicast traffic to be transmitted for multimedia applications throughout a network without being blocked at routed interface (VLAN) boundaries.

ping test A test of the path between the switch and another device on the same or another IP network that can respond to IP packets (ICMP Echo Requests).

PLC Physical layer classification.

PoE Power-over-ethernet. The method by which PDs receive power from a PoE module (operates according to the IEEE 802.3af standard).

PoE + (POEP) Power-over-ethernet plus. The method by which PDs receive power according to the 802.3at standard.

port-number priority The type of power prioritization where, within a priority class, a PoE module assigns the highest priority to the lowestnumbered port in the module, the secondhighest priority to the second lowestnumbered port in the module, and so on.

primary image The software version stored in primary flash on each management module.

priority class The type of power prioritization that uses Low (the default), High, and Critical priority assignments to determine which groups of ports will receive power.

PSAP Public safety answering point. Typically, emergency telephone facilities established as a first point to receive emergency (911) calls and to dispatch emergency response services such as police, fire and emergency medical services.

PSCP PuTTY SCP (see SCP).

PSE Power-sourcing equipment/entity. A PSE, such as a PoE module installed in a switch, provides power to IEEE 802.3afcompliant or IEEE 802.3at-compliant PDs directly connected to the ports on the module.

QoS Quality-of-service. Classifies and prioritizes traffic throughout a network, establishing an end-to-end traffic priority policy to manage available bandwidth and improve throughput of important data.

RADIUS Remote authentication dial-in user service.

rapid switchover stale timer Allows configuration of a timer (in seconds) for Layer 3 forwarding of packets. After failover, the route and neighbor entries in the forwarding information base (FIB) on the active management module are marked as stale. As new routes are added, the stale flag is reset. This continues for the number of seconds indicated by the timer, after which all remaining stale entries are removed.

remote mirroring The monitored (source) interface and exit port in a mirroring session are on different switches. For remote mirroring, you must always configure the IP destination address and exit port (the remote mirroring endpoint) before you configure the monitored interface, by using the following commands:

On the remote (destination) switch: mirror endpoint ip src-ip *`src-udp-port`* *`dst-ip`* *`exit-port`*

On the local (source) switch: mirror *`session`* remote *`ip src-ip`* *`src-udp-port`* *`dst-ip`* [truncation]

RMON Remote monitoring.

SA/DA Source address/destination address.

SCP Secure copy.

secondary image The software version stored in secondary flash on each management module.

selftest A test performed at boot to ensure the management module is functioning correctly. If the module fails selftest, it does not go into active or standby mode. If both modules fail selftest, the switch does not boot.

sFlow Flow sampling. An industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.

sFlow agent A software process that runs as part of the network management software within a device. The agent packages data into datagrams that are forwarded to a central data collector.

sFlow destination The central data collector that gathers datagrams from sFlow-enabled switch ports on the network. The data collector decodes the packet headers and other information to present detailed Layer 2 to Layer 7 usage statistics.

SFTP Secure ftp (file transfer protocol).

SM Standby management module.

SNMP Simple network management protocol. Allows you to manage the switch from a network management station, including support for security features, event reporting, flow sampling, and standard MIBs.

SNTP Simple network time protocol. Synchronizes and ensures a uniform time among interoperating devices.

source switch The source switch on which the inbound and/or outbound traffic to be mirrored originates. See also Monitored Interface.

spoofed ping An ICMP echo request packet intentionally generated with a valid source IP address and an invalid destination IP address. Spoofed pings are often created with the intent to oversubscribe network resources with traffic having invalid destinations.

SSH Secure shell. Provides remote access to management functions on a switch via encrypted paths between the switch and management station clients capable of SSH operation.

SSL Secure socket layer.

SSM System support modules.

standard MTU An IP frame of 1522 bytes in size. (This size includes 4 bytes for the VLAN tag.)

standby management module A management module that is ready to become the active management module if the active management module fails.

STP Spanning tree protocol.

switchover When the other management module becomes the active management module.

syslog Debug/system logging feature.

TCP Transmission control protocol. A transport protocol that runs on IP and is used to set up connections. See also UDP.

TFTP Trivial file transfer protocol. Supports the download of files to the switch from a TFTP network server.

threshold A switch automatically sends all messages created when a system threshold is reached to the network management station that configured the threshold, regardless of the trap receiver configuration.

TLV Type-length-value. A data unit that includes a data type field, a data unit length field (in bytes), and a field containing the actual data the unit is designed to carry (as an alphanumeric string, a bitmap, or a subgroup of information). Some TLVs include subelements that occur as separate data points in displays of information maintained by the switch for LLDP advertisements. (That is, some TLVs include multiple data points or subelements.)

ToS Type of service.

traffic mirroring Intelligent mirroring.

trap receiver Management station to which the switch sends SNMP traps and (optionally) event log messages sent from the switch. From the CLI you can configure up to ten SNMP trap receivers to receive SNMP traps from the switch.

trunk group A set of up to eight ports configured as members of the same port trunk.

TTL Time-to-live.

UDLD Uni-directional link detection. Monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices.

UDP See TCP.

VoIP Voice-over IP.

VRRP Virtual router redundancy protocol. Provides dynamic failover support as backup for gateway IP addresses (first-hop routers) so that if a VR's Master router becomes unavailable, the traffic it supports will be transferred to a backup router without major delays or operator intervention, eliminating single-point-offailure problems.

VT Virus throttling.

warm reboot Binary transfer feature that supports the download of software files from a PC or Unix workstation.

warm standby The active management module does not sync continuously with the standby management module. The standby management module boots to a certain point, syncs basic files, and only finishes booting if the active management module fails or you choose to change which module is the active management module. The transition is not seamless or immediate.

Xmodem Binary transfer feature that supports the download of software files from a PC or Unix workstation.

Index