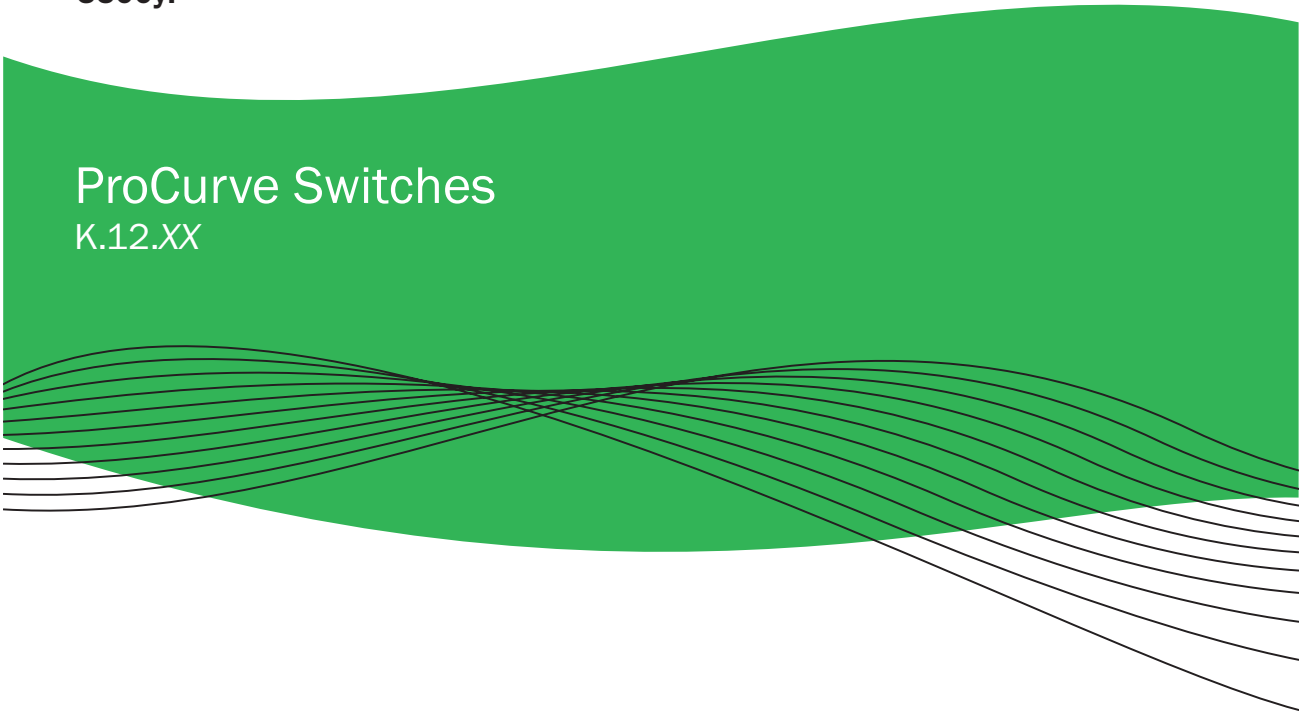
Command Line Interface Reference Guide

6200yl
5400zl
3500yl



ProCurve Switches

K.12.*XX*

www.procurve.com

ProCurve Networking
HP Innovation

Command Line Interface Reference Guide

Series 5400zl Switches
Series 3500yl and 6200yl Switches

Software Release K.12.01

invent

Hewlett-Packard Company

Publication Number

5991-6257

February 2007

Copyright

© Copyright 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Trademark Credits

Microsoft, Windows, Windows 95, and Microsoft Windows NT are US registered trademarks of Microsoft Corporation.

Contents

I. Introduction 11
Introduction 12
Conventions 12
Getting Documentation From the Web 13
CLI Online Help 13
Related Publications 14
How to Navigate This Guide 15
II. Commands 16
aaa 17
Overview 17
Command Structure 17
Examples 21
Command Details 22
access-list 53
Overview 53
arp-protect 56
Overview 56
Command Structure 56
Command Details 57
auto-tftp 59
Overview 59
Command Structure 59
Examples 59
Command Details 59
banner 60
Overview 60
Command Structure 60
Examples 60
Command Details 60
boot 61
Overview 61
Command Structure 61
Examples 61
Command Details 61
cdp 63
Overview 63
Command Structure 63
Examples 63
Command Details 63
chassislocate 64
Overview 64
Command Structure 64
Command Details 64
clear 66
Overview 66
Command Structure 66
Command Details 66
clock 69
Overview 69
Notes 69
Command Structure 69
Command Details 69

© 2007 Hewlett-Packard Development Company, L.P.

configure 72
Overview 72
Command Structure 72
Examples 72
Command Details 72
connection-rate-filter 73
Overview 73
Command Structure 73
Command Details 73
console 75
Overview 75
Command Structure 75
Examples 75
Command Details 76
copy 79
Overview 79
Command Structure 79
Examples 82
Command Details 83
crypto 107
Overview 107
Command Structure 107
Examples 108
Command Details 108
debug 117
Overview 117
Command Structure 117
Command Details 118
dhcp-relay 121
Overview 121
Command Structure 121
Command Details 122
dhcp-snooping 128
Overview 128
Command Structure 128
Command Details 128
dir 133
Overview 133
Command Structure 133
Command Details 133
enable 134
Overview 134
Examples 134
end 135
Overview 135
Notes 135
erase 136
Overview 136
Command Structure 136
Examples 136
Command Details 136
exit 138
Overview 138
Notes 138

© 2007 Hewlett-Packard Development Company, L.P.

Examples 138
fastboot 139
Overview 139
fault-finder 140
Overview 140
Command Structure 140
Command Details 140
filter 142
Overview 142
Command Structure 142
Examples 143
Command Details 143
front-panel-security 147
Overview 147
Command Structure 147
Examples 147
Command Details 147
getMIB 149
Overview 149
Command Structure 149
Command Details 149
gvrp 150
Overview 150
Examples 150
hostname 151
Overview 151
Examples 151
igmp 152
Overview 152
Command Structure 152
Command Details 152
igmp-proxy-domain 153
Overview 153
Command Structure 153
Command Details 153
instrumentation 155
Overview 155
Command Structure 156
Command Details 156
interface 158
Overview 158
Command Structure 158
Command Details 160
ip 180
Overview 180
Command Structure 180
Command Details 182
key-chain 199
Overview 199
Command Structure 199
Examples 202
Command Details 203
kill 224
Overview 224

© 2007 Hewlett-Packard Development Company, L.P.

Notes 224
Command Structure 224
Examples 224
Command Details 225
licenses 226
Overview 226
Command Structure 226
Command Details 226
link-keepalive 228
Overview 228
Command Structure 228
Command Details 228
link-test 229
Overview 229
Command Structure 229
Examples 229
Command Details 230
lldp 231
Overview 231
Command Structure 231
Examples 232
Command Details 232
lockout-mac 238
Overview 238
Notes 238
Examples 238
log 239
Overview 239
Command Structure 239
Command Details 239
logging 241
Overview 241
Command Structure 241
Command Details 241
log-numbers 243
Overview 243
logout 244
Overview 244
loop-protect 245
Overview 245
Command Structure 245
Command Details 245
mac-age-time 247
Overview 247
Examples 247
management-vlan 248
Overview 248
Examples 248
max-vlans 249
Overview 249
Examples 249
menu 250
Overview 250
Examples 250

© 2007 Hewlett-Packard Development Company, L.P.

mesh 251
Overview 251
Command Structure 251
Examples 251
Command Details 251
mirror 252
Overview 252
Command Structure 252
Command Details 253
mirror-port 257
Overview 257
Command Structure 257
Examples 257
Command Details 257
module 259
Overview 259
Command Structure 259
Examples 259
Command Details 259
page 260
Overview 260
password 261
Overview 261
Command Structure 261
Examples 261
Command Details 261
ping 263
Overview 263
Command Structure 263
Examples 263
Command Details 264
port-security 265
Overview 265
Command Structure 266
Examples 266
Command Details 266
power 268
Overview 268
Command Structure 268
Command Details 268
primary-vlan 270
Overview 270
Examples 270
print 271
Overview 271
Command Structure 271
Command Details 271
qos 272
Overview 272
Command Structure 272
Command Details 273
radius-server 282
Overview 282
Command Structure 283

© 2007 Hewlett-Packard Development Company, L.P.

Examples 283
Command Details 284
redo 287
Overview 287
Command Structure 287
Command Details 287
reload 288
Overview 288
Command Structure 288
Examples 288
Command Details 288
rename 290
Overview 290
Command Structure 290
Command Details 290
repeat 291
Overview 291
Command Structure 291
Command Details 291
router 292
Overview 292
Notes 292
Command Structure 292
Command Details 295
setMIB 314
Overview 314
Command Structure 314
Command Details 314
setup 316
Overview 316
Command Structure 316
Examples 316
Command Details 316
sflow 318
Overview 318
Command Structure 318
Command Details 319
show 321
Overview 321
Command Structure 321
Command Details 330
snmp-server 395
Overview 395
Notes 396
Command Structure 397
Examples 398
Command Details 398
snmpv3 404
Overview 404
Command Structure 404
Command Details 405
sntp 413
Overview 413
Command Structure 413

© 2007 Hewlett-Packard Development Company, L.P.

Examples 413
Command Details 413
spanning-tree 415
Overview 415
Command Structure 416
Command Details 418
stack 431
Overview 431
Command Structure 431
Command Details 432
startup-default 433
Overview 433
Command Structure 433
Command Details 433
static-mac 434
Overview 434
Command Structure 434
Examples 434
Command Details 434
static-vlan 436
Overview 436
Examples 436
tacacs-server 437
Overview 437
Command Structure 437
Examples 438
Command Details 438
telnet 440
Overview 440
Command Structure 440
Examples 440
Command Details 440
telnet-server 441
Overview 441
Examples 441
terminal 442
Overview 442
Command Structure 442
Command Details 442
tftp 443
Overview 443
Command Structure 443
Command Details 443
time 444
Overview 444
Command Structure 444
Examples 444
Command Details 445
timesync 447
Overview 447
Command Structure 447
Examples 447
Command Details 447
traceroute 448

© 2007 Hewlett-Packard Development Company, L.P.

Overview 448
Command Structure 448
Examples 448
Command Details 449
trunk 451
Overview 451
Command Structure 451
Examples 451
Command Details 452
update 454
Overview 454
upgrade-software 455
Overview 455
virus-throttle 456
Overview 456
vlan 457
Overview 457
Command Structure 457
Examples 462
Command Details 463
walkMIB 495
Overview 495
Command Structure 495
Examples 495
Command Details 495
web-management 496
Overview 496
Command Structure 496
Examples 497
Command Details 497
write 499
Overview 499
Command Structure 499
Examples 499
Command Details 499

© 2007 Hewlett-Packard Development Company, L.P.

Part I. Introduction

© 2007 Hewlett-Packard Development Company, L.P.

Introduction

CONVENTIONS

Abstract

This guide uses the following conventions for command syntax and displayed information.

Command Syntax Statements

Syntax:

```
aaa port-access authenticator PORT-LIST [ control < authorized | auto |
unauthorized >]
```

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces (< >) enclose required elements.
- Square brackets or braces within square brackets ([< >]) indicate a required element within an optional choice.
- All caps 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:

  Syntax:

  ```
  aaa port-access authenticator PORT-LIST
  ```

Command Prompts

In the default configuration the Series 5400zl switches, for example, display one of the following CLI prompts:

- ProCurve Switch 5406zl#
- ProCurve Switch 5412zl#

To simplify recognition, this guide uses ProCurve or HPswitch to represent command prompts for all models. For example:

```
ProCurve#

HPswitch#
```

(You can use the hostname command to change the text in the CLI prompt.)

© 2007 Hewlett-Packard Development Company, L.P.

Example Commands

Example commands and their output appear in the Courier type face. For example:

```
ProCurve(config)# clear public-key
ProCurve(config)# show ip client-public-key
show_client_public_key: cannot stat keyfile
```

Port Numbering Conventions

ProCurve chassis switches designate individual ports with a letter/number combination to show the slot in which the port is found and the sequential number the port has in that slot (A1, A2, B1, B2, etc.)

GETTING DOCUMENTATION FROM THE WEB

You need the Adobe® Acrobat® Reader to view, print, and/or copy ProCurve Networking product documentation.

1. Go to the ProCurve Networking Web site at **www.procurve.com** [http://www.procurve.com.]
2. Click on Technical support, then Product manuals(all).
3. Click on the name of the product for which you want documentation.
4. On the resulting Web page, double-click on a document you want to view or download.

CLI ONLINE HELP

To access the online help, type the command, followed by a space, then press the [Tab] key.

List Available Commands

Type "?" to list available commands. Typing the ? symbol lists the commands you can execute at the current privilege level.

Use [Tab] to search for or complete a command word. You can use [Tab] to help you find CLI commands or to quickly complete the current word in a command. To do so, type one or more consecutive characters in a command and then press [Tab] (with no spaces allowed). Pressing [Tab] after a completed command word lists the further options for that command.

Options Available in Current Context

You can use the CLI to remind you of the options available for a command by entering command keywords followed by ?.

Displaying Command-List Help

Syntax: help

Displays a listing of command help summaries for all commands available at the current privilege level. That is, at the Operator level, executing help displays the help summaries only for Operator-Level commands. At the Manager level, executing help displays the help summaries for both the Operator and Manager levels, and so on.

Displaying Help for an Individual Command

Syntax: COMMAND-STRING help

© 2007 Hewlett-Packard Development Company, L.P.

This option displays help for any command available at the current context level.

RELATED PUBLICATIONS

The following documents (available on the ProCurve website) provide additional information on the CLI commands.

Software Release Notes

Release notes provide information on new software updates:

- New features and how to configure and use them
- Software management, including downloading software to the switch
- Software fixes addressed in current and previous releases

Product Notes and Software Update Information

The printed Read Me First shipped with your switch provides product notes and other information.

Installation and Getting Started Guide

Use the Installation and Getting Started Guide shipped with your switch to prepare for and perform the physical installation. This guide also steps you through connecting the switch to your network and assigning IP addressing, and describes the LED indications for correct operation and trouble analysis. A PDF version of this guide is also provided on the Product Documentation CD-ROM shipped with the switch. And you can download a copy from the ProCurve website.

Management and Configuration Guide

Use the Management and Configuration Guide for information on:

- Using the command line (CLI), Menu interface, and web browser interface
- Memory and configuration operation
- IP addressing
- Time protocols
- Port configuration, trunking, traffic control, and PoE operation
- SNMP, LLDP, and other network management topics
- File transfers, switch monitoring, troubleshooting, and MAC address management

Access Security Guide

Use the Access Security Guide to learn how to use and configure the following access security features available in the switch:

- Local username and password security
- Web-based and MAC-based authentication
- RADIUS and TACACS+ authentication
- SSH (Secure Shell) and SSL (Secure Socket Layer) operation
- 802.1X access control
- Port security operation with MAC-based control
- Authorized IP Manager security
- Access Control Lists (ACLs)
- KMS (Key Management System)

© 2007 Hewlett-Packard Development Company, L.P.

Advanced Traffic Management Guide

Use the Advanced Traffic Management Guide for information on:

- VLANs: Static port-based and protocol VLANs, and dynamic GVRP VLANs
- Spanning-Tree: 802.1D (STP), 802.1w (RSTP), and 802.1s (MSTP)
- meshing
- Quality-of-Service (QoS)

Multicast and Routing Guide

Use the Multicast and Routing Guide for information on:

- IGMP
- PIM (SM and DM)
- IP routing
- VRRP

HOW TO NAVIGATE THIS GUIDE

The commands and page numbers in this guide are hyperlinked in blue to allow you to easily navigate to the desired command detail. Hyperlinked areas are:

- Overview: Related commands section
- Command Structure
- Command Details summary listing
- Next Available Options within individual command options and parameters
- Page numbers displayed with commands

When the hand cursor is positioned over a blue hyperlinked area, the hand displays a pointing finger. Left-click once to go the the indicated command. Additionally, the Command Details section lists the commands in alphabetical order.

Navigating Printed Copy

If you are using a printed copy of this guide, use the page numbers displayed at the end of a command, option, or parameter to go to the desired command detail.

Traversing the Command Structure

The commands shown in the Command Structure section of a chapter mimic the command organization of the switch. For example, if you select the command "aaa", one of the next command options is "accounting". The next available option under accounting is "commands". The Command Structure provides a high-level view of all the command options and parameters for that command. Each of these is hyperlinked to take you to the details about that option or parameter.

© 2007 Hewlett-Packard Development Company, L.P.

Part II. Commands

© 2007 Hewlett-Packard Development Company, L.P.

aaa

OVERVIEW

Category:	802.1X, Accounting, Switch Security
Primary context:	config
Related Commands	**show authentication (page 335)** **show port-access (page 371)** **show accounting (page 333)** **show radius (page 375)** **show tacacs (page 384)** **radius-server (page 282)** **tacacs-server (page 437)**

```
Usage: aaa <...>

Description: Configure the switch Authentication, Authorization, and Accounting
             features. Use 'aaa ?' command to see a list of all possible
             configuration options.
```

COMMAND STRUCTURE

- [no] aaa **accounting** -- Configure accounting parameters on the switch **(p. 23)**
  - **commands** -- Configure 'commands' type of accounting **(p. 29)**
    - **mode < stop-only >** -- Specify how to initiate and terminate an accounting session. **(p. 36)**
      - **method < radius >** -- Specify which accounting method to use (radius) **(p. 36)**
  - **exec** -- Configure 'exec' type of accounting **(p. 31)**
    - **mode < start-stop | stop-only >** -- Specify how to initiate and terminate an accounting session. **(p. 36)**
      - **method < radius >** -- Specify which accounting method to use (radius) **(p. 36)**
  - **network** -- Configure 'network' type of accounting **(p. 37)**
    - **mode < start-stop | stop-only >** -- Specify how to initiate and terminate an accounting session. **(p. 36)**
      - **method < radius >** -- Specify which accounting method to use (radius) **(p. 36)**
  - **suppress** -- Do not generate accounting records for a specific type of user. **(p. 47)**
    - **null-username** -- Do not generate accounting records for users with a null-username. **(p. 38)**
  - **system** -- Configure 'system' type of accounting **(p. 47)**
    - **mode < start-stop | stop-only >** -- Specify how to initiate and terminate an accounting session. **(p. 36)**
      - **method < radius >** -- Specify which accounting method to use (radius) **(p. 36)**
  - **update** -- Configure update accounting records mechanism **(p. 48)**
    - **periodic < 1 to 525600 >** -- Configure update accounting records mechanism **(p. 38)**
- [no] aaa **authentication** -- Configure authentication parameters on the switch **(p. 24)**
  - **console** -- Configure authentication mechanism used to control access to the switch console **(p. 29)**
    - **enable** -- Configure access to the privileged mode commands. **(p. 30)**
      - **primary < local | tacacs | radius >** -- Specify the primary authentication method for access control. **(p. 40)**
        - **secondary < local | none >** -- Specify the backup authentication method for access control. **(p. 43)**
    - **login** -- Configure login access to the switch. **(p. 32)**

© 2007 Hewlett-Packard Development Company, L.P.

- **primary < local | tacacs | radius >** -- Specify the primary authentication method for access control. **(p. 40)**
  - **secondary < local | none >** -- Specify the backup authentication method for access control. **(p. 43)**
- **login** -- Specify that switch respects the authentication server's privilege level **(p. 32)**
  - **privilege-mode** -- Specify that switch respects the authentication server's privilege level **(p. 42)**
- **num-attempts < 1 to 10 >** -- Specify the maximum number of login attempts allowed **(p. 38)**
- **port-access** -- Configure authentication mechanism used to control access to the network **(p. 38)**
  - **chap-radius** -- Use CHAP (MD5) capable RADIUS server for 802.1x authentication. **(p. 28)**
  - **eap-radius** -- Use EAP capable RADIUS server for 802.1x authentication. **(p. 30)**
  - **local** -- Use the switch operator user name and password for 802.1x authentication. **(p. 32)**
- **ssh** -- Configure authentication mechanism used to control SSH access to the switch **(p. 45)**
  - **enable** -- Configure access to the privileged mode commands. **(p. 30)**
    - **primary < local | tacacs | radius | ... >** -- Specify the primary authentication method for access control. **(p. 40)**
      - **secondary < local | none >** -- Specify the backup authentication method for access control. **(p. 43)**
  - **login** -- Configure login access to the switch. **(p. 32)**
    - **primary < local | tacacs | radius | ... >** -- Specify the primary authentication method for access control. **(p. 40)**
      - **secondary < local | none >** -- Specify the backup authentication method for access control. **(p. 43)**
- **telnet** -- Configure authentication mechanism used to control telnet access to the switch **(p. 47)**
  - **enable** -- Configure access to the privileged mode commands. **(p. 30)**
    - **primary < local | tacacs | radius >** -- Specify the primary authentication method for access control. **(p. 40)**
      - **secondary < local | none >** -- Specify the backup authentication method for access control. **(p. 43)**
  - **login** -- Configure login access to the switch. **(p. 32)**
    - **primary < local | tacacs | radius >** -- Specify the primary authentication method for access control. **(p. 40)**
      - **secondary < local | none >** -- Specify the backup authentication method for access control. **(p. 43)**
- **web** -- Configure authentication mechanism used to control web access to the switch **(p. 49)**
  - **enable** -- Configure access to the privileged mode commands. **(p. 30)**
    - **primary < local | radius >** -- Specify the primary authentication method for access control. **(p. 40)**
      - **secondary < local | none >** -- Specify the backup authentication method for access control. **(p. 43)**
  - **login** -- Configure login access to the switch. **(p. 32)**
    - **primary < local | radius >** -- Specify the primary authentication method for access control. **(p. 40)**
      - **secondary < local | none >** -- Specify the backup authentication method for access control. **(p. 43)**

■ [no] aaa **authorization** -- Configure authorization parameters on the switch **(p. 27)**
- **commands** -- Configure exec (shell) commands authorization. **(p. 29)**
  - **primary_method < radius | none >** -- **(p. 42)**

■ [no] aaa **port-access** -- Configure 802 **(p. 38)**
- **authenticator** -- Configure 802 **(p. 25)**
  - **active** -- Activate/deactivate 802.1x authenticator. **(p. 24)**

© 2007 Hewlett-Packard Development Company, L.P.

- **PORT-LIST** -- Manage 802.1x on the device port(s). ([ethernet] PORT-LIST) **(p. 39)**
  - **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default). **(p. 28)**
    - **VLAN-ID** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 49)**
  - **clear-statistics** -- Clear the authenticator statistics. **(p. 28)**
  - **client-limit** -- Set the maximum number of clients to allow on the port. **(p. 28)**
    - **NUMBER-OF-CLIENTS < 1 to 32 >** -- Set the maximum number of clients to allow on the port. (NUMBER) **(p. 38)**
  - **control < authorized | auto | unauthorized >** -- Set the authenticator to Force Authorized, Force Unauthorized or Auto state (default Auto). (NUMBER) **(p. 30)**
  - **initialize** -- Reinitialize the authenticator state machine. **(p. 32)**
  - **logoff-period < 1 to 999999999 >** -- Set period of time after which a client will be considered removed from the port for a lack of activity. (NUMBER) **(p. 33)**
  - **max-requests < 1 to 10 >** -- Set maximum number of times the switch retransmits authentication requests (default 2). (NUMBER) **(p. 35)**
  - **quiet-period < 0 to 65535 >** -- Set the period of time the switch does not try to acquire a supplicant (default 60 sec.). (NUMBER) **(p. 42)**
  - **reauthenticate** -- Force re-authentication to happen. **(p. 43)**
  - **reauth-period < 0 to 9999999 >** -- Set the re-authentication timeout (in seconds, default 0); set to '0' to disable re-authentication. (NUMBER) **(p. 43)**
  - **server-timeout < 1 to 300 >** -- Set the authentication server response timeout (default 30sec.). (NUMBER) **(p. 44)**
  - **supplicant-timeout < 1 to 300 >** -- Set the supplicant response timeout on an EAP request (default 30 sec.). (NUMBER) **(p. 46)**
  - **tx-period < 1 to 65535 >** -- Set the period of time the switch waits until retransmission of EAPOL PDU (default 30 sec.). (NUMBER) **(p. 48)**
  - **unauth-period < 0 to 255 >** -- Set period of time the switch waits for authentication before moving the port to the VLAN for unauthenticated clients. (NUMBER) **(p. 48)**
  - **unauth-vid** -- Configures VLAN where to keep port while there is an unauthenticated client connected (not configured by default). **(p. 48)**
    - **VLAN-ID** -- Configures VLAN where to keep port while there is an unauthenticated client connected (not configured by default). (VLAN-ID) **(p. 49)**
- **mac-based** -- Configure MAC address based network authentication on the device or the device's port(s) **(p. 33)**
  - **addr-format < no-delimiter | single-dash | multi-dash | ... >** -- Set the MAC address format to be used in the RADIUS request message (default no-delimiter). **(p. 24)**
  - **mac-list1** -- Manage MAC address based network authentication on the device port(s). ([ethernet] PORT-LIST) **(p. 35)**
    - **addr-limit < 1 to 32 >** -- Set the port's maximum number of authenticated MAC addresses (default 1). (NUMBER) **(p. 24)**
    - **addr-moves** -- Set whether the MAC can move between ports (default disabled - no moves). **(p. 24)**
    - **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default). **(p. 28)**
      - **VLAN-ID** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 49)**
    - **logoff-period < 1 to 9999999 >** -- Set the period of time of inactivity that the switch considers an implicit logoff (default 300 seconds). (NUMBER) **(p. 33)**
    - **max-requests < 1 to 10 >** -- Set maximum number of times the switch retransmits authentication requests (default 3). (NUMBER) **(p. 35)**
    - **quiet-period < 1 to 65535 >** -- Set the period of time the switch does not try to authenticate (default 60 seconds). (NUMBER) **(p. 42)**

© 2007 Hewlett-Packard Development Company, L.P.

- **reauthenticate** -- Force re-authentication to happen. **(p. 43)**
- **reauth-period < 0 to 9999999 >** -- Set the re-authentication timeout in seconds; set to '0' to disable re-authentication (default 0). (NUMBER) **(p. 43)**
- **server-timeout < 1 to 300 >** -- Set the authentication server response timeout (default 30 seconds). (NUMBER) **(p. 44)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). **(p. 48)**
  - **VLAN-ID** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). (VLAN-ID) **(p. 49)**

- **PORT-LIST** -- Manage general port security features on the device port(s). ([ethernet] PORT-LIST) **(p. 39)**
  - **controlled-direction < both | in >** -- Configure how traffic is controlled on non-authenticated ports; in BOTH directions (ingress+egress) or IN only (ingress). (NUMBER) **(p. 30)**
- **supplicant** -- Manage 802 ([ethernet] PORT-LIST) **(p. 45)**
  - **auth-timeout < 1 to 300 >** -- Set the challenge reception timeout (default 30sec.). (NUMBER) **(p. 28)**
  - **clear-statistics** -- Clear the supplicant statistics. **(p. 28)**
  - **held-period < 0 to 65535 >** -- Set the held period (default 60sec.). (NUMBER) **(p. 32)**
  - **identity** -- Set the identity(user name) to be used by the supplicant. (ASCII-STR) **(p. 32)**
    - **secret** -- **(p. 44)**
  - **initialize** -- Reinitialize the supplicant state machine. **(p. 32)**
  - **max-start < 1 to 10 >** -- Define the maximum number of attempts taken to start authentication (default 3). (NUMBER) **(p. 36)**
  - **secret** -- Trigger the command to ask user for a password for the supplicant to use. **(p. 44)**
  - **start-period < 1 to 300 >** -- Set a period of time between EAPOL-Start packet retransmission (default 30sec.). (NUMBER) **(p. 45)**
- **web-based** -- Configure web authentiation based network authentication on the device or the device's port(s) **(p. 50)**
  - **dhcp-addr** -- Set the base address / mask for the temporary pool used by DHCP (base address default is 192.168.0.0, mask default is 24 - 255.255.255.0). (IP-ADDR/MASK-LENGTH) **(p. 30)**
  - **dhcp-lease < 5 to 25 >** -- Set the lease length of the IP address issued by DHCP (default 10). (NUMBER) **(p. 30)**
  - **web-list1** -- Manage web authentication based network authentication on the device port(s). ([ethernet] PORT-LIST) **(p. 52)**
    - **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default). **(p. 28)**
      - **web-authvid** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 50)**
    - **client-limit < 1 to 32 >** -- Set the port's maximum number of authenticated clients (default 1). (NUMBER) **(p. 28)**
    - **client-moves** -- Set whether the client can move between ports (default disabled - no moves). **(p. 29)**
    - **logoff-period < 1 to 9999999 >** -- Set the period of time of inactivity that the switch considers an implicit logoff (default 300 seconds). (NUMBER) **(p. 33)**
    - **max-requests < 1 to 10 >** -- Set maximum number of times the switch retransmits authentication requests (default 3). (NUMBER) **(p. 35)**
    - **max-retries < 1 to 10 >** -- Set number of times a client can enter their credentials before authentication is considered to have failed (default 3). (NUMBER) **(p. 36)**
    - **quiet-period < 1 to 65535 >** -- Set the period of time the switch does not try to authenticate (default 60 seconds). (NUMBER) **(p. 42)**
    - **reauthenticate** -- Force re-authentication to happen. **(p. 43)**
    - **reauth-period < 0 to 9999999 >** -- Set the re-authentication timeout in seconds; set to '0' to disable re-authentication (default 0). (NUMBER) **(p. 43)**

© 2007 Hewlett-Packard Development Company, L.P.

- **redirect-url** -- Set the URL that the user should be redirected to after successful login (default none), Specify url up to 103 characters length. **(p. 43)**
  - **web-redirect-url** -- Set the URL that the user should be redirected to after successful login (default none), Specify url up to 103 characters length. (ASCII-STR) **(p. 52)**
- **server-timeout < 1 to 300 >** -- Set the authentication server response timeout (default 30 seconds). (NUMBER) **(p. 44)**
- **ssl-login** -- Set whether to enable SSL login (https on port 443) (default disabled). **(p. 45)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). **(p. 48)**
  - **web-unauthvid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). (VLAN-ID) **(p. 52)**

EXAMPLES

Example: aaa

The following examples show access options, and the corresponding commands to configure them.

Authenticate console enable (Manager) access, using TACACS+ as the primary method and the switch's local database as the secondary method:

```
ProCurve(config)# aaa authentication console enable tacacs local
```

Authenticate Telnet login (Operator) access, using TACACS+ as the primary method and the switch's local database as the secondary method:

```
ProCurve(config)# aaa authentication Telnet login tacacs local
```

Authenticate Telnet login (Manager) access, using TACACS+ as the primary method and the switch's local database as the secondary method:

```
ProCurve(config)# aaa authentication telnet enable tacacs local
```

Deny access and terminate a session after two consecutive failures to provide the correct username and password:

```
ProCurve(config)# aaa authentication num-attempts 2
```

Example: aaa authentication

If you already configured local passwords on the switch, but want RADIUS to protect primary Telnet and SSH access without allowing a secondary Telnet or SSH access option (the switch's local passwords), type the following commands:

© 2007 Hewlett-Packard Development Company, L.P.

```
HPswitch(config)# aaa authentication telnet login radius none
HPswitch(config)# aaa authentication telnet enable radius none
HPswitch(config)# aaa authentication ssh login radius none
HPswitch(config)# aaa authentication ssh enable radius none
HPswitch(config)# show authentication
 Status and Counters - Authentication Information
  Login Attempts : 3
  Respect Privilege : Disabled

              | Login      Login      Enable     Enable
  Access Task | Primary    Secondary  Primary    Secondary
  ----------- + ---------- ---------- ---------- ----------
  Console     | Local      None       Local      None
  Telnet      | Radius     None       Radius     None
  Port-Access | Local
  Webui       | Local      None       Local      None
  SSH         | Radius     None       Radius     None
  Web-Auth    | ChapRadius
  MAC-Auth    | ChapRadius
```

Example: aaa authentication port-access eap-radius

Configure the switch for 802.1X authentication using an EAP-RADIUS server:

```
ProCurve(config)# aaa authentication port-access eap-radius
```

Example: aaa port-access authenticator

Configure ports A10 - A20 as 802.1X authenticator ports:

```
ProCurve(config)# aaa port-access authenticator a10-a20
```

Example: aaa port-access authenticator active

Activate 802.1X port-access on ports you have configured as authenticators:

```
ProCurve(config)# aaa port-access authenticator active
```

Example: aaa port-access authenticator auth-vid

Configure ports A10 - A20 to use VLAN 81 as the Authorized-Client VLAN:

```
ProCurve(config)# aaa port-access authenticator e a10-a20 auth-vid 81
```

Example: aaa port-access authenticator unauth-vid

Configure ports A10 - A20 to use VLAN 80 as the Unauthorized-Client VLAN:

```
ProCurve(config)# aaa port-access authenticator e a10-a20 unauth-vid 80
```

COMMAND DETAILS

accounting (p. 23)
active (p. 24)
addr-format (p. 24)
addr-limit (p. 24)
addr-moves (p. 24)
authentication (p. 24)
authenticator (p. 25)
authorization (p. 27)
auth-timeout (p. 28)
identity (p. 32)
initialize (p. 32)
local (p. 32)
login (p. 32)
logoff-period (p. 33)
mac-based (p. 33)
mac-list1 (p. 35)
max-requests (p. 35)
max-retries (p. 36)
reauth-period (p. 43)
redirect-url (p. 43)
secondary (p. 43)
secret (p. 44)
server-timeout (p. 44)
ssh (p. 45)
ssl-login (p. 45)
start-period (p. 45)
supplicant (p. 45)

© 2007 Hewlett-Packard Development Company, L.P.

auth-vid (p. 28)	max-start (p. 36)	supplicant-timeout (p. 46)
chap-radius (p. 28)	method (p. 36)	suppress (p. 47)
clear-statistics (p. 28)	mode (p. 36)	system (p. 47)
client-limit (p. 28)	network (p. 37)	telnet (p. 47)
client-moves (p. 29)	null-username (p. 38)	tx-period (p. 48)
commands (p. 29)	num-attempts (p. 38)	unauth-period (p. 48)
console (p. 29)	NUMBER-OF-CLIENTS (p. 38)	unauth-vid (p. 48)
control (p. 30)	periodic (p. 38)	update (p. 48)
controlled-direction (p. 30)	port-access (p. 38)	VLAN-ID (p. 49)
dhcp-addr (p. 30)	PORT-LIST (p. 39)	web (p. 49)
dhcp-lease (p. 30)	primary (p. 40)	web-authvid (p. 50)
eap-radius (p. 30)	primary_method (p. 42)	web-based (p. 50)
enable (p. 30)	privilege-mode (p. 42)	web-list1 (p. 52)
exec (p. 31)	quiet-period (p. 42)	web-redirect-url (p. 52)
held-period (p. 32)	reauthenticate (p. 43)	web-unauthvid (p. 52)

accounting

- aaa accounting

```
Usage: [no] aaa accounting <exec|network|system|commands>
                           <start-stop|stop-only>
                           <radius>
       [no] aaa accounting update periodic <number>
       [no] aaa accounting suppress

Description: Configure the switch to use a RADIUS server for accounting of
             user access. The first option of the command specifies
             a type of accounting, how an accounting session will be started and
             ended, and the method used for accounting. The second option sets
             the accounting update period for all accouting sessions on the switch.
             The "no" form disables the update function and resets the value to
             zero. (Default: zero)
             The third option disables accounting for unknown users having no
             username.
Parameters:
            o exec       - Provides information about user EXEC terminal
                           sessions (user shells) on the switch.
            o network    - Provides information about 8021x sessions.
            o system     - Provides information about all system-level events,
                           such as the system reboots or accounting turned
                           on/off.
            o commands   - Provides information about commands executed on the
                           switch.
            o start-stop - Send a start record accounting notice at the
                           beginning and a stop record notice at the end of the
                           accounting session. Do not wait for acknowledgement.
            o stop-only  - Send a stop record accounting notice at the end of
                           the accounting session.Do not wait for
                           acknowledgement.
            o radius     - Use RADIUS as the accounting protocol
                           accounting information is available.
            o update periodic <number> - Send accounting update records at
                           regular intervals given by 'number' (in minutes).
            o suppress   - suppress accounting when a user with
                           no username accesses the switch
```

Next Available Options:

- **commands** -- Configure 'commands' type of accounting**(p. 29)**
- **exec** -- Configure 'exec' type of accounting**(p. 31)**
- **network** -- Configure 'network' type of accounting**(p. 37)**
- **suppress** -- Do not generate accounting records for a specific type of user. **(p. 47)**
- **system** -- Configure 'system' type of accounting**(p. 47)**
- **update** -- Configure update accounting records mechanism**(p. 48)**

active

- [no] aaa port-access authenticator active

```
Activate/deactivate 802.1x authenticator.
```

addr-format

- aaa port-access mac-based addr-format *< no-delimiter | single-dash | multi-dash | ... >*

```
Set the MAC address format to be used in the RADIUS request message (default
no-delimiter).
```

Supported Values:
- **no-delimiter** -- no delimiter format: AABBCCDDEEFF.
- **single-dash** -- single dash format: AABBCC-DDEEFF.
- **multi-dash** -- multi-dash format: AA-BB-CC-DD-EE-FF.
- **multi-colon** -- multi-colon format: AA:BB:CC:DD:EE:FF.

addr-limit

- aaa port-access mac-based *[ETHERNET] PORT-LIST* addr-limit *< 1 to 32 >*

```
Set the port's maximum number of authenticated MAC addresses (default 1).
```

Range: < 1 to 32 >

addr-moves

- [no] aaa port-access mac-based *[ETHERNET] PORT-LIST* addr-moves

```
Set whether the MAC can move between ports (default disabled - no moves).
```

authentication

- aaa authentication

```
Usage: aaa authentication ...

Description: Configure authentication for Console, Telnet, SSH or Web.
             The command configures the authentication mechanism used to
             control access the switch resources. For each access type, you
             can configure authentication separately for login (Operator) or
             enable Manager access.
             You can specify a primary authentication method and, optionally,
             a secondary method to try if the first method fails to check the
             user's credentials.
             Use 'aaa authentication' command to see a list of all possible
             configuration options.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **console** -- Configure authentication mechanism used to control access to the switch console**(p. 29)**
- **telnet** -- Configure authentication mechanism used to control telnet access to the switch**(p. 47)**
- **web** -- Configure authentication mechanism used to control web access to the switch**(p. 49)**
- **ssh** -- Configure authentication mechanism used to control SSH access to the switch**(p. 45)**
- **port-access** -- Configure authentication mechanism used to control access to the network**(p. 38)**
- **num-attempts** < 1 to 10 > -- Specify the maximum number of login attempts allowed**(p. 38)**
- **login** -- Specify that switch respects the authentication server's privilege level**(p. 32)**

authenticator

- aaa port-access authenticator

```
Usage:  [no] aaa port-access authenticator active

        [no] aaa port-access authenticator [ethernet] PORT-LIST
        [control <authorized|auto|unauthorized> | quiet-period <0-65535> |
         tx-period <1-65535> | supplicant-timeout <1-300> |
         server-timeout <1-300> | max-requests <1-10> |
         reauth-period <0-9999999> | auth-vid VLAN-ID | unauth-vid VLAN-ID |
         unauth-period <0-255> | logoff-period <1-999999999> |
         client-limit [<1-32>] |
         controlled-directions <in|both> |
         initialize | reauthenticate | clear-statistics]

Description: Configure 802.1x (Port Based Network Access) authentication
             on the device or the device's port(s).

             The first form of the command activates or deactivates
             authentication on the device. By default, authentication is
             deactivated. 802.1x authentication does not run on the switch
             until you use this command to enable it.

             The second form of the command enables, disables, or
             configures authentication on the device's individual ports.

             While authentication is deactivated, access to the network
             is granted on all switch ports regardless of whether
             802.1x is enabled on the port.

             The 'no' keyword cannot be used with any of the optional
             parameters that follow PORT-LIST.

             802.1x must be enabled on a port before any of the following
             optional parameters can be configured on the port.

             o 'control' sets the authenticator to (Force) Authorized,
               (Force) Unauthorized or Auto state (default 'Auto').
               - Auto: Grants network access to a connected device that
                       supports 802.1x authentication and provides valid
                       credentials.
               - Authorized: Grants access to any devices connected to
                       the port(s). In this case, the devices do not have
                       to provide 802.1x credentials or support 802.1x
                       authentication. (Also termed ''Force Authorized''.)
```

© 2007 Hewlett-Packard Development Company, L.P.

```
    - Unauthorized: In this state, the port blocks access to
            any connected device, regardless of whether the
            device provides the correct credentials and has
            802.1x support.
```

- 'quiet-period' sets the period of time during which the switch does not try to acquire a supplicant after a failed authentication attempt(default 60 seconds).
- 'tx-period' sets the period of time the switch waits to retransmit the next EAPOL PDU during an authentication session (default 30 seconds).
- 'server-timeout' sets the period of time after which the switch assumes that authentication has timed out (default 30 seconds).
- 'supp-timeout' sets the period of time after which the switch decides that a supplicant has not responded to an EAP request (default 30 seconds).
- 'max-requests' sets maximum number of times the switch retransmits a request to the backend authentication system (RADIUS server) before closing the current authentication session (default 2).
- 'reauth-period' sets the period of time after which connected clients must be re-authenticated. When the timeout is set to 0 the re-authentication is disabled (default 0 seconds).
- 'auth-vid' configures the VLAN to which to move port after successful authentication. RADIUS server can override the value. Use 'no' form of the command to set this PVID to 0. If the PVID set to 0 no PVID changes occure unless RADIUS server requests. Changes take effect after client reauthentication. The default is 0.
- 'unauth-vid' configures the VLAN to which to move port if an unauthorized client has been connected on the port and there is no other client on the port. The switch will wait for the amount of time specified as the 'unauth-period' before the port will be moved to this VLAN. If the port PVID successfully set to the value configured, the port becomes unblocked and the client can communicate to other members of this VLAN. Use 'no' form of the command to set this PVID to 0. Changes take effect immediately. The default is 0.
- 'unauth-period' sets period of time the switch waits for authentication before assigning the 'unauth-vid' to the port if an unauthenticated client has been detected on this port. The default is 0 seconds.
- 'logoff-period' sets period of time after which a client will be considered removed from the port for a lack of activity. The default is 300 seconds.
- 'client-limit' sets the maximum number of clients to allow on the port. This includes ALL clients (authenticated and unauthenticated).

© 2007 Hewlett-Packard Development Company, L.P.

```
      NOTE: No more than 32 unique client MAC addresses can be
            authorized by both 802.1x and MAC/web-based
            authentication together on the same port.
      The 'no... client-limit' command allows unlimited number of
      clients on the port. Authenticator makes no distinction between
      clients and operates port as a single protocol entity with
      no specific MAC address filter on the port.
      The default is no client limit.

    o 'controlled-directions' configures how traffic is controlled
      on non-authenticated ports.
      - Both: (default)  In this mode, ingress+egress traffic
              to/from a non-authenticated port is controlled.
              For all practical purposes, only traffic related
              to the authentication process itself is allowed to
              pass through.
      - In:   In this mode, ingress traffic is controlled (in the
              same way as in 'both' mode; that is, only traffic
              related to authentication is allowed to pass).
              Traffic in the egress direction is not controlled
              by the authenticator.  This mode is very useful, for
              example, to a network administrator who wishes to
              deploy authentication and Wake-on-LAN.

              Note:  in order for a port to operationally be
                     in the 'in' mode, this port must also be an
                     edge port ('spanning-tree <port> edge-port');
                     this port's MAC must be functional (this port
                     must have link); and a BPDU must not be seen
                     on this port.

    o 'initialize' re-initialize authentication on the specified
      ports. That is, 'initialize' blocks inbound and outbound
      traffic and restarts the authentication process on the
      specified ports that are configured with 'control auto' (see
      the 'control' parameter, described above) and actively
      operating as authenticators.

    o 'reauthenticate' forces re-authentication (unless the
      authenticator is in 'HELD' state).

    o 'clear-statistics' clears authenticator statistics
      counters.
```

Next Available Options:

- **PORT-LIST** -- Manage 802.1x on the device port(s). ([ethernet] PORT-LIST) **(p. 39)**
- **active** -- Activate/deactivate 802.1x authenticator.**(p. 24)**

authorization

- aaa authorization

```
Usage: [no] aaa authorization <commands> <radius>

Description: Configure authorization parameters on the switch.
```

Next Available Option:

- **commands** -- Configure exec (shell) commands authorization. **(p. 29)**

© 2007 Hewlett-Packard Development Company, L.P.

auth-timeout

- aaa port-access supplicant *[ETHERNET] PORT-LIST* auth-timeout *< 1 to 300 >*

  ```
  Set the challenge reception timeout (default 30sec.).
  ```

  Range: < 1 to 300 >

auth-vid

- [no] aaa port-access authenticator *[ETHERNET] PORT-LIST* auth-vid

  ```
  Configures VLAN where to move port after successful authentication (not configured
  by default).
  ```

  Next Available Option:
  - **VLAN-ID** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 49)**

- [no] aaa port-access mac-based *[ETHERNET] PORT-LIST* auth-vid

  ```
  Configures VLAN where to move port after successful authentication (not configured
  by default).
  ```

  Next Available Option:
  - **VLAN-ID** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 49)**

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* auth-vid

  ```
  Configures VLAN where to move port after successful authentication (not configured
  by default).
  ```

  Next Available Option:
  - **web-authvid** -- Configures VLAN where to move port after successful authentication (not configured by default). (VLAN-ID) **(p. 50)**

chap-radius

- aaa authentication port-access chap-radius

  ```
  Use CHAP (MD5) capable RADIUS server for 802.1x authentication.
  ```

clear-statistics

- aaa port-access authenticator *[ETHERNET] PORT-LIST* clear-statistics

  ```
  Clear the authenticator statistics.
  ```

- aaa port-access supplicant *[ETHERNET] PORT-LIST* clear-statistics

  ```
  Clear the supplicant statistics.
  ```

client-limit

- [no] aaa port-access authenticator *[ETHERNET] PORT-LIST* client-limit

© 2007 Hewlett-Packard Development Company, L.P.

```
Set the maximum number of clients to allow on the port.
```

Next Available Option:

- **NUMBER-OF-CLIENTS** < 1 to 32 > -- Set the maximum number of clients to allow on the port. (NUMBER) **(p. 38)**

- aaa port-access web-based *[ETHERNET] PORT-LIST* client-limit *< 1 to 32 >*

```
Set the port's maximum number of authenticated clients (default 1).
```

Range: < 1 to 32 >

client-moves

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* client-moves

```
Set whether the client can move between ports (default disabled - no moves).
```

commands

- [no] aaa accounting commands

```
Usage: [no] aaa accounting commands <stop-only> <radius>

Description: Configure 'commands' type of accounting.
Parameters:
            o stop-only - Send a record accounting notice after the execution
                          of command.
            o radius    - Use RADIUS as the accounting protocol.
```

Next Available Option:

- **mode** < stop-only > -- Specify how to initiate and terminate an accounting session. **(p. 36)**

- [no] aaa authorization commands

```
Configure exec (shell) commands authorization.
```

Next Available Option:

- **primary_method** < radius | none > -- **(p. 42)**

console

- aaa authentication console

```
Usage: aaa authentication console <enable|login>
                                  <primary-method> [<backup-method>]

Description: Configure authentication mechanism used to control access
             to the switch console.
Parameters:
            o enable           - Configure access to privileged mode.
            o login            - Configure login access.
            o <primary-method> - Specifies the primary authentication
                                 method for access control. Use <TAB>
                                 or <?> after you specify enable or login
                                 to get a list of all available
                                 primary authentication methods.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
o <backup-method> -  Specifies an authentication method
                     to use, if the primary authentication
                     method is not able to check user's
                     credentials.
                     Use <TAB> or <?> after you specify the
                     primary authentication method to get a list
                     of all available backup methods.
```

Next Available Options:

- **enable** -- Configure access to the privileged mode commands.**(p. 30)**
- **login** -- Configure login access to the switch.**(p. 32)**

control

- aaa port-access authenticator *[ETHERNET] PORT-LIST* control *< authorized | auto | unauthorized >*

```
Set the authenticator to Force Authorized, Force
Unauthorized or Auto state (default Auto).
```

Supported Values:

- **authorized** -- Force authorized.
- **auto** -- Auto.
- **unauthorized** -- Force unauthorized.

controlled-direction

- aaa port-access *[ETHERNET] PORT-LIST* controlled-direction *< both | in >*

```
Configure how traffic is controlled on non-authenticated ports; in
BOTH directions (ingress+egress) or IN only (ingress).
```

Supported Values:

- **both** -- Exert control in both directions.
- **in** -- Exert control on incoming packets.

dhcp-addr

- aaa port-access web-based dhcp-addr *IP-ADDR/MASK-LENGTH*

```
Set the base address / mask for the temporary pool used by DHCP (base address default
 is 192.168.0.0, mask default is 24 - 255.255.255.0).
```

dhcp-lease

- aaa port-access web-based dhcp-lease *< 5 to 25 >*

```
Set the lease length of the IP address issued by DHCP (default 10).
```

Range: < 5 to 25 >

eap-radius

- aaa authentication port-access eap-radius

```
Use EAP capable RADIUS server for 802.1x authentication.
```

enable

- aaa authentication console enable

© 2007 Hewlett-Packard Development Company, L.P.

```
Configure access to the privileged mode commands.
```

Next Available Option:

- **primary** < local | tacacs | radius > -- Specify the primary authentication method for access control.**(p. 40)**

■ aaa authentication telnet enable

```
Configure access to the privileged mode commands.
```

Next Available Option:

- **primary** < local | tacacs | radius > -- Specify the primary authentication method for access control.**(p. 40)**

■ aaa authentication web enable

```
Configure access to the privileged mode commands.
```

Next Available Option:

- **primary** < local | radius > -- Specify the primary authentication method for access control.**(p. 40)**

■ aaa authentication ssh enable

```
Configure access to the privileged mode commands.
```

Next Available Option:

- **primary** < local | tacacs | radius | ... > -- Specify the primary authentication method for access control.**(p. 40)**

exec

■ [no] aaa accounting exec

```
Usage: [no] aaa accounting exec <start-stop|stop-only>
                                <radius>

Description: Configure 'exec' type of accounting.
Parameters:
            o start-stop - Send a start record accounting notice at the
                           beginning and a stop record notice at the end
                           of the accounting session. Do not wait for
                           acknowledgement.
            o stop-only  - Send a stop record accounting notice at the end
                           of the accounting session.Do not wait for
                           acknowledgement.
            o radius     - Use RADIUS as the accounting protocol
```

Next Available Option:

- **mode** < start-stop | stop-only > -- Specify how to initiate and terminate an accounting session. **(p. 36)**

© 2007 Hewlett-Packard Development Company, L.P.

held-period

- aaa port-access supplicant *[ETHERNET] PORT-LIST* held-period *< 0 to 65535 >*

  ```
  Set the held period (default 60sec.).
  ```

  Range: < 0 to 65535 >

identity

- aaa port-access supplicant *[ETHERNET] PORT-LIST* identity *IDENTITY*

  ```
  Set the identity(user name) to be used by the supplicant.
  ```

  Next Available Option:
  - **secret** -- **(p. 44)**

initialize

- aaa port-access authenticator *[ETHERNET] PORT-LIST* initialize

  ```
  Reinitialize the authenticator state machine.
  ```

- aaa port-access supplicant *[ETHERNET] PORT-LIST* initialize

  ```
  Reinitialize the supplicant state machine.
  ```

local

- aaa authentication port-access local

  ```
  Use the switch operator user name and password for 802.1x authentication.
  ```

login

- aaa authentication console login

  ```
  Configure login access to the switch.
  ```

  Next Available Option:
  - **primary** < local | tacacs | radius > -- Specify the primary authentication method for access control.**(p. 40)**

- aaa authentication telnet login

  ```
  Configure login access to the switch.
  ```

  Next Available Option:
  - **primary** < local | tacacs | radius > -- Specify the primary authentication method for access control.**(p. 40)**

- aaa authentication web login

  ```
  Configure login access to the switch.
  ```

  Next Available Option:
  - **primary** < local | radius > -- Specify the primary authentication method for access control.**(p. 40)**

© 2007 Hewlett-Packard Development Company, L.P.

- aaa authentication ssh login

```
Configure login access to the switch.
```

Next Available Option:

- **primary** < local | tacacs | radius | ... > -- Specify the primary authentication method for access control.**(p. 40)**

- aaa authentication login

```
Usage: [no] aaa authentication login privilege-mode

Description: Specify that switch respects the
             authentication server's privilege level.
```

Next Available Option:

- **privilege-mode** -- Specify that switch respects the authentication server's privilege level**(p. 42)**

logoff-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* logoff-period *< 1 to 999999999 >*

```
Set period of time after which a client will be considered removed from the
port for a lack of activity.
```

Range: < 1 to 999999999 >

- aaa port-access mac-based *[ETHERNET] PORT-LIST* logoff-period *< 1 to 9999999 >*

```
Set the period of time of inactivity that the switch considers an implicit logoff
(default 300 seconds).
```

Range: < 1 to 9999999 >

- aaa port-access web-based *[ETHERNET] PORT-LIST* logoff-period *< 1 to 9999999 >*

```
Set the period of time of inactivity that the switch considers an implicit logoff
(default 300 seconds).
```

Range: < 1 to 9999999 >

mac-based

- aaa port-access mac-based

```
Usage:  [no] aaa port-access mac-based
         addr-format <no-delimiter | single-dash | multi-dash | multi-colon>

        [no] aaa port-access mac-based [ethernet] PORT-LIST
        [addr-limit <1-32> | addr-moves | quiet-period <1-65535> |
         server-timeout <1-300> | max-requests <1-10> |
         logoff-period <1-9999999> | reauth-period <0-9999999>
         auth-vid VLAN-ID | unauth-vid VLAN-ID |
         controlled-direction <in|both> | reauthenticate]

Description: Configure MAC address based network authentication
             on the device or the device's port(s).

             The first form of the command sets the
```

```
MAC address format which is common to all ports

The second form of the command enables, disables, or
configures authentication on the device's individual ports.

o 'addr-format' sets the MAC address format to be used in the
  RADIUS request message (default no-delimiter).

o 'addr-limit' sets the maximum number of MAC addresses to
  allow on the port. This includes ALL addresses (authenticated
  and unauthenticated). The default is 1 MAC address.
  NOTE: No more than 32 unique client MAC addresses can be
        authorized by both 802.1x and MAC/web-based
        authentication together on the same port.

o 'addr-moves' sets whether the MAC address can move
  between ports that also have 'addr-moves' enabled
  (default disabled - no moves allowed).

o 'quiet-period' sets the period of time during which the
  switch does not try to authenticate after a failed
  authentication attempt (default 60 seconds).

o 'server-timeout' sets the period of time after which the
  switch assumes that authentication has timed out
  (default 30 seconds).

o 'max-requests' sets the number of authentication attempts
  that must time out before authentication fails (default 3).

o 'logoff-period' sets the period of time of inactivity that
  the switch considers an implicit logoff (default 300).

o 'reauth-period' sets the period of time after which connected
  MAC addresses must be re-authenticated.  When set to 0
  the re-authentication is disabled (default 0).

o 'auth-vid' configures the VLAN to which to move a port
  after successful authentication.  RADIUS server can
  override the value.  Use 'no' form of the command to set
  this PVID to 0.  If the PVID is set to 0 no PVID changes
  occur unless RADIUS server requests.  Changes take effect
  immediately.  All clients must immediately re-authenticate.
  The default is 0.

o 'unauth-vid' configures the VLAN to which to move a port
  after failed authentication.  Use 'no' form of the command
  to set this PVID to 0.  Changes take effect immediately.
  The default is 0.

o 'controlled-directions' configures how traffic is controlled
  on non-authenticated ports.
  - Both: (default)  In this mode, ingress+egress traffic
          to/from a non-authenticated port is controlled.
          For all practical purposes, only traffic related
          to the authentication process itself is allowed to
          pass through.
  - In:   In this mode, ingress traffic is controlled (in the
          same way as in 'both' mode; that is, only traffic
          related to authentication is allowed to pass).
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                    Traffic in the egress direction is not controlled
                    by the authenticator.  This mode is very useful, for
                    example, to a network administrator who wishes to
                    deploy authentication and Wake-on-LAN.

                    Note:  in order for a port to operationally be in the
                           'in' mode, this port must also be an edge port
                           ('spanning-tree <port> admin-edge-port');
                           this port's MAC must be functional (this port
                           must have link); and a BPDU must not be seen
                           on this port.

              o 'reauthenticate' forces re-authentication
                of all clients present on a port.
```

Next Available Options:

- **mac-list1** -- Manage MAC address based network authentication on the device port(s). ([ethernet] PORT-LIST) **(p. 35)**
- **addr-format** < no-delimiter | single-dash | multi-dash | ... > -- Set the MAC address format to be used in the RADIUS request message (default no-delimiter).**(p. 24)**

mac-list1

- [no] aaa port-access mac-based *[ETHERNET] PORT-LIST*

```
Manage MAC address based network authentication on the device port(s).
```

Next Available Options:

- **addr-limit** < 1 to 32 > -- Set the port's maximum number of authenticated MAC addresses (default 1). (NUMBER) **(p. 24)**
- **addr-moves** -- Set whether the MAC can move between ports (default disabled - no moves).**(p. 24)**
- **logoff-period** < 1 to 9999999 > -- Set the period of time of inactivity that the switch considers an implicit logoff (default 300 seconds). (NUMBER) **(p. 33)**
- **quiet-period** < 1 to 65535 > -- Set the period of time the switch does not try to authenticate (default 60 seconds). (NUMBER) **(p. 42)**
- **server-timeout** < 1 to 300 > -- Set the authentication server response timeout (default 30 seconds). (NUMBER) **(p. 44)**
- **max-requests** < 1 to 10 > -- Set maximum number of times the switch retransmits authentication requests (default 3). (NUMBER) **(p. 35)**
- **reauth-period** < 0 to 9999999 > -- Set the re-authentication timeout in seconds; set to '0' to disable re-authentication (default 0). (NUMBER) **(p. 43)**
- **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default).**(p. 28)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default).**(p. 48)**
- **reauthenticate** -- Force re-authentication to happen.**(p. 43)**

max-requests

- aaa port-access authenticator *[ETHERNET] PORT-LIST* max-requests *< 1 to 10 >*

```
Set maximum number of times the switch retransmits
authentication requests (default 2).
```

© 2007 Hewlett-Packard Development Company, L.P.

Range: < 1 to 10 >

- aaa port-access mac-based *[ETHERNET] PORT-LIST* max-requests *< 1 to 10 >*

```
Set maximum number of times the switch retransmits authentication requests (default
3).
```

Range: < 1 to 10 >

- aaa port-access web-based *[ETHERNET] PORT-LIST* max-requests *< 1 to 10 >*

```
Set maximum number of times the switch retransmits authentication requests (default
3).
```

Range: < 1 to 10 >

max-retries

- aaa port-access web-based *[ETHERNET] PORT-LIST* max-retries *< 1 to 10 >*

```
Set number of times a client can enter their credentials before authentication is
considered to have failed (default 3).
```

Range: < 1 to 10 >

max-start

- aaa port-access supplicant *[ETHERNET] PORT-LIST* max-start *< 1 to 10 >*

```
Define the maximum number of attempts taken to start authentication
(default 3).
```

Range: < 1 to 10 >

method

- aaa accounting commands *< stop-only > < radius >*

```
Specify which accounting method to use (radius)
```

Supported Values:
- **radius** -- Use RADIUS protocol as accounting method.

- aaa accounting exec *< start-stop | stop-only > < radius >*

```
Specify which accounting method to use (radius)
```

Supported Values:
- **radius** -- Use RADIUS protocol as accounting method.

- aaa accounting network *< start-stop | stop-only > < radius >*

```
Specify which accounting method to use (radius)
```

Supported Values:
- **radius** -- Use RADIUS protocol as accounting method.

- aaa accounting system *< start-stop | stop-only > < radius >*

```
Specify which accounting method to use (radius)
```

Supported Values:
- **radius** -- Use RADIUS protocol as accounting method.

mode

- aaa accounting commands *< stop-only >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Specify how to initiate and terminate an accounting session.
```

Supported Values:
- **stop-only** -- Send stop record accounting notice.

Next Available Option:
- **method** < radius > -- Specify which accounting method to use (radius) **(p. 36)**

■ aaa accounting exec *< start-stop | stop-only >*

```
Specify how to initiate and terminate an accounting session.
```

Supported Values:
- **start-stop** -- Send start and stop record accounting notice.
- **stop-only** -- Send stop record accounting notice only.

Next Available Option:
- **method** < radius > -- Specify which accounting method to use (radius) **(p. 36)**

■ aaa accounting network *< start-stop | stop-only >*

```
Specify how to initiate and terminate an accounting session.
```

Supported Values:
- **start-stop** -- Send start and stop record accounting notice.
- **stop-only** -- Send stop record accounting notice only.

Next Available Option:
- **method** < radius > -- Specify which accounting method to use (radius) **(p. 36)**

■ aaa accounting system *< start-stop | stop-only >*

```
Specify how to initiate and terminate an accounting session.
```

Supported Values:
- **start-stop** -- Send start and stop record accounting notice.
- **stop-only** -- Send stop record accounting notice only.

Next Available Option:
- **method** < radius > -- Specify which accounting method to use (radius) **(p. 36)**

network

■ [no] aaa accounting network

```
Usage: [no] aaa accounting network <start-stop|stop-only>
                                   <radius>

Description: Configure 'network' type of accounting.
Parameters:
            o start-stop - Send a start record accounting notice at the
                           beginning and a stop record notice at the end
                           of the accounting session. Do not wait for
                           acknowledgement.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
              o stop-only  - Send a stop record accounting notice at the end
                             of the accounting session.Do not wait for
                             acknowledgement.
              o radius     - Use RADIUS as the accounting protocol
```

Next Available Option:

- **mode** < start-stop | stop-only > -- Specify how to initiate and terminate an accounting session. **(p. 36)**

null-username

- [no] aaa accounting suppress null-username

```
Do not generate accounting records for users with a null-username.
```

num-attempts

- aaa authentication num-attempts *< 1 to 10 >*

```
Usage: aaa authentication num-attempts <1-10>

Description: Specify the maximum number of login attempts
             allowed. The default value is 3.
```

Range: < 1 to 10 >

NUMBER-OF-CLIENTS

- aaa port-access authenticator *[ETHERNET] PORT-LIST* client-limit *< 1 to 32 >*

```
Set the maximum number of clients to allow on the port.
```

Range: < 1 to 32 >

periodic

- aaa accounting update periodic *< 1 to 525600 >*

```
Usage: [no] aaa accounting update periodic <number>

Description: Configure update accounting records mechanism.
Parameters:
            periodic <number> - Send accounting update records at regular
                                intervals given by 'number' (in minutes).
```

Range: < 1 to 525600 >

port-access

- aaa authentication port-access

```
Usage: aaa authentication port-access ...

Description: Configure authentication mechanism used to control access
             to the network. The configured authentication method will.
             be used to authenticate 802.1x (Port Based Network Access
             Control Protocol) clients. The command should be followed
             by a keyword identifying an authentication method
             to use for Port Based Network Access Control Protocol clients
             authentication. Use 'aaa authentication port-access ?'
             to get a list of all available authentication methods.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:
- **local** -- Use the switch operator user name and password for 802.1x authentication.**(p. 32)**
- **eap-radius** -- Use EAP capable RADIUS server for 802.1x authentication.**(p. 30)**
- **chap-radius** -- Use CHAP (MD5) capable RADIUS server for 802.1x authentication.**(p. 28)**

■ aaa port-access

```
Usage: [no] aaa port-access <authenticator ... | supplicant ...
                            web-based ... | mac-based ...>

Description: Configure 802.1x (Port Based Network Access),
             MAC address based network access,
             or web authentication based network access
             on the device.  You can configure authenticator,
             supplicant, MAC address based, or web authentication based
             network access on the device or device ports by specifying
             a corresponding keyword.
             See 'aaa port-access authenticator help', 'aaa port-access
             supplicant help', 'aaa port-access mac-based help', and
             'aaa port-access web-based help' for further details on
             authenticator, supplicant, MAC address based, and
             web authentication based network access configuration.
```

Next Available Options:
- **authenticator** -- Configure 802**(p. 25)**
- **supplicant** -- Manage 802 ([ethernet] PORT-LIST) **(p. 45)**
- **mac-based** -- Configure MAC address based network authentication on the device or the device's port(s)**(p. 33)**
- **web-based** -- Configure web authentiation based network authentication on the device or the device's port(s)**(p. 50)**
- **PORT-LIST** -- Manage general port security features on the device port(s). ([ethernet] PORT-LIST) **(p. 39)**

PORT-LIST

■ [no] aaa port-access authenticator *[ETHERNET] PORT-LIST*

```
Manage 802.1x on the device port(s).
```

Next Available Options:
- **control** < authorized | auto | unauthorized > -- Set the authenticator to Force Authorized, Force Unauthorized or Auto state (default Auto). (NUMBER) **(p. 30)**
- **quiet-period** < 0 to 65535 > -- Set the period of time the switch does not try to acquire a supplicant (default 60 sec.). (NUMBER) **(p. 42)**
- **tx-period** < 1 to 65535 > -- Set the period of time the switch waits until retransmission of EAPOL PDU (default 30 sec.). (NUMBER) **(p. 48)**
- **supplicant-timeout** < 1 to 300 > -- Set the supplicant response timeout on an EAP request (default 30 sec.). (NUMBER) **(p. 46)**
- **server-timeout** < 1 to 300 > -- Set the authentication server response timeout (default 30sec.). (NUMBER) **(p. 44)**
- **max-requests** < 1 to 10 > -- Set maximum number of times the switch retransmits authentication requests (default 2). (NUMBER) **(p. 35)**
- **reauth-period** < 0 to 9999999 > -- Set the re-authentication timeout (in seconds, default 0); set to '0' to disable re-authentication. (NUMBER) **(p. 43)**

© 2007 Hewlett-Packard Development Company, L.P.

- **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default).**(p. 28)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthenticated client connected (not configured by default).**(p. 48)**
- **unauth-period** < 0 to 255 > -- Set period of time the switch waits for authentication before moving the port to the VLAN for unauthenticated clients. (NUMBER) **(p. 48)**
- **logoff-period** < 1 to 999999999 > -- Set period of time after which a client will be considered removed from the port for a lack of activity. (NUMBER) **(p. 33)**
- **client-limit** -- Set the maximum number of clients to allow on the port.**(p. 28)**
- **initialize** -- Reinitialize the authenticator state machine.**(p. 32)**
- **reauthenticate** -- Force re-authentication to happen.**(p. 43)**
- **clear-statistics** -- Clear the authenticator statistics.**(p. 28)**

■ [no] aaa port-access *[ETHERNET] PORT-LIST*

```
Manage general port security features on the device port(s).
```

Next Available Option:
- **controlled-direction** < both | in > -- Configure how traffic is controlled on non-authenticated ports; in BOTH directions (ingress+egress) or IN only (ingress). (NUMBER) **(p. 30)**

primary

■ aaa authentication console enable *< local | tacacs | radius >*

```
Specify the primary authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.
- **radius** -- Use RADIUS server.

Next Available Option:
- **secondary** < local | none > -- Specify the backup authentication method for access control.**(p. 43)**

■ aaa authentication console login *< local | tacacs | radius >*

```
Specify the primary authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.
- **radius** -- Use RADIUS server.

Next Available Option:
- **secondary** < local | none > -- Specify the backup authentication method for access control.**(p. 43)**

■ aaa authentication telnet enable *< local | tacacs | radius >*

```
Specify the primary authentication method for access control.
```

© 2007 Hewlett-Packard Development Company, L.P.

Supported Values:
- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.
- **radius** -- Use RADIUS server.

Next Available Option:
- **secondary** < local | none > -- Specify the backup authentication method for access control.**(p. 43)**

- aaa authentication telnet login *< local | tacacs | radius >*

```
Specify the primary authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.
- **radius** -- Use RADIUS server.

Next Available Option:
- **secondary** < local | none > -- Specify the backup authentication method for access control.**(p. 43)**

- aaa authentication web enable *< local | radius >*

```
Specify the primary authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **radius** -- Use RADIUS server.

Next Available Option:
- **secondary** < local | none > -- Specify the backup authentication method for access control.**(p. 43)**

- aaa authentication web login *< local | radius >*

```
Specify the primary authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **radius** -- Use RADIUS server.

Next Available Option:
- **secondary** < local | none > -- Specify the backup authentication method for access control.**(p. 43)**

- aaa authentication ssh enable *< local | tacacs | radius | ... >*

```
Specify the primary authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.

© 2007 Hewlett-Packard Development Company, L.P.

- **radius** -- Use RADIUS server.
- **public-key** -- Use local switch public key authentication database.

Next Available Option:
- **secondary** < local | none > -- Specify the backup authentication method for access control.**(p. 43)**

■ aaa authentication ssh login *< local | tacacs | radius | ... >*

```
Specify the primary authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **tacacs** -- Use TACACS+ server.
- **radius** -- Use RADIUS server.
- **public-key** -- Use local switch public key authentication database.

Next Available Option:
- **secondary** < local | none > -- Specify the backup authentication method for access control.**(p. 43)**

primary_method

■ aaa authorization commands *< radius | none >*

Supported Values:
- **radius** -- Use RADIUS protocol as the authorization method.
- **none** -- No authorization (always succeeds).

privilege-mode

■ [no] aaa authentication login privilege-mode

```
Usage: [no] aaa authentication login privilege-mode

Description: Specify that switch respects the
             authentication server's privilege level.
```

quiet-period

■ aaa port-access authenticator *[ETHERNET] PORT-LIST* quiet-period *< 0 to 65535 >*

```
Set the period of time the switch does not try to
acquire a supplicant (default 60 sec.).
```

Range: < 0 to 65535 >

■ aaa port-access mac-based *[ETHERNET] PORT-LIST* quiet-period *< 1 to 65535 >*

```
Set the period of time the switch does not try to authenticate (default 60 seconds).
```

Range: < 1 to 65535 >

■ aaa port-access web-based *[ETHERNET] PORT-LIST* quiet-period *< 1 to 65535 >*

```
Set the period of time the switch does not try to authenticate (default 60 seconds).
```

Range: < 1 to 65535 >

© 2007 Hewlett-Packard Development Company, L.P.

reauthenticate

- aaa port-access authenticator *[ETHERNET] PORT-LIST* reauthenticate

```
Force re-authentication to happen.
```

- aaa port-access mac-based *[ETHERNET] PORT-LIST* reauthenticate

```
Force re-authentication to happen.
```

- aaa port-access web-based *[ETHERNET] PORT-LIST* reauthenticate

```
Force re-authentication to happen.
```

reauth-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* reauth-period *< 0 to 9999999 >*

```
Set the re-authentication timeout (in seconds,
default 0); set to '0' to disable re-authentication.
```

Range: < 0 to 9999999 >

- aaa port-access mac-based *[ETHERNET] PORT-LIST* reauth-period *< 0 to 9999999 >*

```
Set the re-authentication timeout in seconds; set to '0' to disable re-authentication
 (default 0).
```

Range: < 0 to 9999999 >

- aaa port-access web-based *[ETHERNET] PORT-LIST* reauth-period *< 0 to 9999999 >*

```
Set the re-authentication timeout in seconds; set to '0' to disable re-authentication
 (default 0).
```

Range: < 0 to 9999999 >

redirect-url

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* redirect-url

```
Set the URL that the user should be redirected to after successful login (default
none), Specify url up to 103 characters length.
```

Next Available Option:

- **web-redirect-url** -- Set the URL that the user should be redirected to after successful login (default none), Specify url up to 103 characters length. (ASCII-STR) **(p. 52)**

secondary

- aaa authentication console enable *< local | tacacs | radius >* *< local | none >*

```
Specify the backup authentication method for access control.
```

Supported Values:

- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.

- aaa authentication console login *< local | tacacs | radius >* *< local | none >*

```
Specify the backup authentication method for access control.
```

Supported Values:

© 2007 Hewlett-Packard Development Company, L.P.

- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.

■ aaa authentication telnet enable *< local | tacacs | radius > < local | none >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.

■ aaa authentication telnet login *< local | tacacs | radius > < local | none >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.

■ aaa authentication web enable *< local | radius > < local | none >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.

■ aaa authentication web login *< local | radius > < local | none >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.

■ aaa authentication ssh enable *< local | tacacs | radius | ... > < local | none >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.

■ aaa authentication ssh login *< local | tacacs | radius | ... > < local | none >*

```
Specify the backup authentication method for access control.
```

Supported Values:
- **local** -- Use local switch user/password database.
- **none** -- Do not use backup authentication methods.

secret

■ aaa port-access supplicant *[ETHERNET] PORT-LIST* identity *IDENTITY* secret

■ aaa port-access supplicant *[ETHERNET] PORT-LIST* secret

```
Trigger the command to ask user for a password for the supplicant to use.
```

server-timeout

■ aaa port-access authenticator *[ETHERNET] PORT-LIST* server-timeout *< 1 to 300 >*

```
Set the authentication server response timeout (default 30sec.).
```

© 2007 Hewlett-Packard Development Company, L.P.

Range: < 1 to 300 >

- aaa port-access mac-based *[ETHERNET] PORT-LIST* server-timeout *< 1 to 300 >*

```
Set the authentication server response timeout (default 30 seconds).
```

Range: < 1 to 300 >

- aaa port-access web-based *[ETHERNET] PORT-LIST* server-timeout *< 1 to 300 >*

```
Set the authentication server response timeout (default 30 seconds).
```

Range: < 1 to 300 >

ssh

- aaa authentication ssh

```
Usage: aaa authentication ssh <enable|login>
                                <primary-method> [<backup-method>]

Description: Configure authentication mechanism used to control SSH
             access to the switch.
Parameters:
            o enable           - Configure access to privileged mode.
            o login            - Configure login access.
            o <primary-method> - Specifies the primary authentication
                                 method for access control. Use <TAB>
                                 or <?> after you specify enable or login
                                 to get a list of all available
                                 primary authentication methods.
            o <backup-method> -  Specifies an authentication method
                                 to use, if the primary authentication
                                 method is not able to check user's
                                 credentials.
                                 Use <TAB> or <?> after you specify the
                                 primary authentication method to get a list
                                 of all available backup methods.
```

Next Available Options:

- **enable** -- Configure access to the privileged mode commands.**(p. 30)**
- **login** -- Configure login access to the switch.**(p. 32)**

ssl-login

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* ssl-login

```
Set whether to enable SSL login (https on port 443) (default disabled).
```

start-period

- aaa port-access supplicant *[ETHERNET] PORT-LIST* start-period *< 1 to 300 >*

```
Set a period of time between EAPOL-Start packet retransmission
(default 30sec.).
```

Range: < 1 to 300 >

supplicant

- [no] aaa port-access supplicant *[ETHERNET] PORT-LIST*

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] aaa port-access supplicant [ethernet] PORT-LIST
       [auth-timeout <1-300> | held-period <0-65535> |
        start-period <1-300> | max-start <1-10> |
        identity <identity> [secret] | secret
        initialize | reauthenticate | clear-statistics]

Description: Manage 802.1x (Port Based Network Access) supplicant
             on the device ports. Called without the optional parameters
             the command enables or disables (if 'no' is specified) the
             supplicant functionality on the specified ports.
             The 'no' keyword can not be used with any of the
             optional parameters. All changes made by the command apply
             to the specified PORT-LIST only.
             o 'auth-timeout' sets the period of time the supplicant waits
               to receive a challenge from the authenticator
               (default 30sec.).
             o 'held-period' sets a period of time the supplicant waits
               after receiving a failure before trying to re-acquire the
               authenticatior (default 60sec.).
             o 'start-period' sets a period of time between transmitting
               EAPOL-Start packets in Connecting state (default 30sec.).
             o 'max-start' defines the maximum number of attempts to
               start authentication before the supplicant assumes that
               it has been authenticated (default 3).
             o 'identity' sets the identity to be used by the port
               supplicant when MD5 authentication request is received
               from an authenticator.
             o 'secret' sets the secret to be used by the port
               supplicant when MD5 authentication request is received
               from an authenticator. User will be prompted to enter
               the secret after the command is invoked.
             o 'initialize' reinitializes supplicant's state machine.
             o 'clear-statistics' clears supplicant statistics counters.
```

Next Available Options:

- **auth-timeout** < 1 to 300 > -- Set the challenge reception timeout (default 30sec.). (NUMBER) **(p. 28)**
- **held-period** < 0 to 65535 > -- Set the held period (default 60sec.). (NUMBER) **(p. 32)**
- **start-period** < 1 to 300 > -- Set a period of time between EAPOL-Start packet retransmission (default 30sec.). (NUMBER) **(p. 45)**
- **max-start** < 1 to 10 > -- Define the maximum number of attempts taken to start authentication (default 3). (NUMBER) **(p. 36)**
- **initialize** -- Reinitialize the supplicant state machine.**(p. 32)**
- **identity** -- Set the identity(user name) to be used by the supplicant. (ASCII-STR) **(p. 32)**
- **secret** -- Trigger the command to ask user for a password for the supplicant to use.**(p. 44)**
- **clear-statistics** -- Clear the supplicant statistics.**(p. 28)**

supplicant-timeout

- aaa port-access authenticator *[ETHERNET] PORT-LIST* supplicant-timeout *< 1 to 300 >*

```
Set the supplicant response timeout on an EAP request
(default 30 sec.).
```

Range: < 1 to 300 >

suppress

- [no] aaa accounting suppress

```
Do not generate accounting records for a specific type of user.
```

Next Available Option:

- **null-username** -- Do not generate accounting records for users with a null-username. **(p. 38)**

system

- [no] aaa accounting system

```
Usage: [no] aaa accounting system  <start-stop|stop-only>
                                   <radius>

Description: Configure 'system' type of accounting.
Parameters:
            o start-stop - Send a start record accounting notice at the
                           beginning and a stop record notice at the end
                           of the accounting session. Do not wait for
                           acknowledgement.
            o stop-only  - Send a stop record accounting notice at the end
                           of the accounting session.Do not wait for
                           acknowledgement.
            o radius     - Use RADIUS as the accounting protocol
```

Next Available Option:

- **mode** < start-stop | stop-only > -- Specify how to initiate and terminate an accounting session. **(p. 36)**

telnet

- aaa authentication telnet

```
Usage: aaa authentication telnet <enable|login>
                                 <primary-method> [<backup-method>]

Description: Configure authentication mechanism used to control telnet
             access to the switch.
Parameters:
            o enable           - Configure access to privileged mode.
            o login            - Configure login access.
            o <primary-method> - Specifies the primary authentication
                                 method for access control. Use <TAB>
                                 or <?> after you specify enable or login
                                 to get a list of all available
                                 primary authentication methods.
            o <backup-method> -  Specifies an authentication method
                                 to use, if the primary authentication
                                 method is not able to check user's
                                 credentials.
                                 Use <TAB> or <?> after you specify the
                                 primary authentication method to get a list
                                 of all available backup methods.
```

Next Available Options:

- **enable** -- Configure access to the privileged mode commands.**(p. 30)**

© 2007 Hewlett-Packard Development Company, L.P.

- **login** -- Configure login access to the switch.**(p. 32)**

tx-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* tx-period *< 1 to 65535 >*

```
Set the period of time the switch waits until
retransmission of EAPOL PDU (default 30 sec.).
```

Range: < 1 to 65535 >

unauth-period

- aaa port-access authenticator *[ETHERNET] PORT-LIST* unauth-period *< 0 to 255 >*

```
Set period of time the switch waits for authentication before moving the
port to the VLAN for unauthenticated clients.
```

Range: < 0 to 255 >

unauth-vid

- [no] aaa port-access authenticator *[ETHERNET] PORT-LIST* unauth-vid

```
Configures VLAN where to keep port while there is an unauthenticated client connected
 (not configured by default).
```

Next Available Option:

- **VLAN-ID** -- Configures VLAN where to keep port while there is an unauthenticated client connected (not configured by default). (VLAN-ID) **(p. 49)**

- [no] aaa port-access mac-based *[ETHERNET] PORT-LIST* unauth-vid

```
Configures VLAN where to keep port while there is an unauthorized client connected
(not configured by default).
```

Next Available Option:

- **VLAN-ID** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). (VLAN-ID) **(p. 49)**

- [no] aaa port-access web-based *[ETHERNET] PORT-LIST* unauth-vid

```
Configures VLAN where to keep port while there is an unauthorized client connected
(not configured by default).
```

Next Available Option:

- **web-unauthvid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default). (VLAN-ID) **(p. 52)**

update

- [no] aaa accounting update

```
Usage: [no] aaa accounting update periodic <number>

Description: Configure update accounting records mechanism.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
Parameters:
            periodic <number> - Send accounting update records at regular
                                intervals given by 'number' (in minutes).
```

Next Available Option:

- **periodic** < 1 to 525600 > -- Configure update accounting records mechanism**(p. 38)**

VLAN-ID

- aaa port-access authenticator *[ETHERNET] PORT-LIST* auth-vid *VLAN-ID*

```
Configures VLAN where to move port after successful authentication (not configured
by default).
```

- aaa port-access authenticator *[ETHERNET] PORT-LIST* unauth-vid *VLAN-ID*

```
Configures VLAN where to keep port while there is an unauthenticated client connected
 (not configured by default).
```

- aaa port-access mac-based *[ETHERNET] PORT-LIST* auth-vid *VLAN-ID*

```
Configures VLAN where to move port after successful authentication (not configured
by default).
```

- aaa port-access mac-based *[ETHERNET] PORT-LIST* unauth-vid *VLAN-ID*

```
Configures VLAN where to keep port while there is an unauthorized client connected
(not configured by default).
```

web

- aaa authentication web

```
Usage: aaa authentication web <enable|login>
                                <primary-method> [<backup-method>]

Description: Configure authentication mechanism used to control web
             access to the switch.
Parameters:
            o enable           - Configure access to privileged mode.
            o login            - Configure login access.
            o <primary-method> - Specifies the primary authentication
                                 method for access control. Use <TAB>
                                 or <?> after you specify enable or login
                                 to get a list of all available
                                 primary authentication methods.
            o <backup-method> -  Specifies an authentication method
                                 to use, if the primary authentication
                                 method is not able to check user's
                                 credentials.
                                 Use <TAB> or <?> after you specify the
                                 primary authentication method to get a list
                                 of all available backup methods.
```

Next Available Options:

- **enable** -- Configure access to the privileged mode commands.**(p. 30)**
- **login** -- Configure login access to the switch.**(p. 32)**

© 2007 Hewlett-Packard Development Company, L.P.

web-authvid

- aaa port-access web-based *[ETHERNET] PORT-LIST* auth-vid *VLAN-ID*

```
Configures VLAN where to move port after successful authentication (not configured
by default).
```

web-based

- aaa port-access web-based

```
Usage:  [no] aaa port-access web-based
        [dhcp-addr <base address / mask> | dhcp-lease <5-25>]

        [no] aaa port-access web-based [ethernet] PORT-LIST
        [client-limit <1-32> | client-moves | ssl-login |
         redirect-url <URL> | quiet-period <1-65535> |
         server-timeout <1-300> | max-requests <1-10> |
         max-retries <1-10> | logoff-period <1-9999999> |
         reauth-period <0-9999999> | auth-vid VLAN-ID |
         unauth-vid VLAN-ID | controlled-direction <in|both> |
         reauthenticate]

Description: Configure web authentiation based network authentication
             on the device or the device's port(s).

             The first form of the command sets the dhcp address
             or lease parameter which are common to all ports

             The second form of the command enables, disables, or
             configures authentication on the device's individual ports.

             o 'dhcp-addr' sets the base address / mask for the temporary
               pool used by DHCP (base address default is 192.168.0.0,
               mask default is 24 - 255.255.255.0)

             o 'dhcp-lease' sets the lease length of the temporary
               IP address issued by DHCP (default 10)

             o 'client-limit' sets the maximum number of clients to allow on
               the port. This includes ALL clients (authenticated and
               unauthenticated). The default is 1 client.
               NOTE: No more than 32 unique client MAC addresses can be
                     authorized by both 802.1x and MAC/web-based
                     authentication together on the same port.

             o 'client-moves' sets whether the client can move
               between ports that also have 'client-moves' enabled
               (default disabled - no moves allowed).

             o 'ssl-login' sets whether to enable SSL logins (https on
               port 443).  If enabled, logins to plaintext http (port 80)
               are redirected to https port.  The default is disabled.

             o 'redirect-url' sets the URL that the user should be
               redirected to after successful login (default none)
               Specify url up to 103 characters length.

             o 'quiet-period' sets the period of time during which the
               switch does not try to authenticate after a failed
```

© 2007 Hewlett-Packard Development Company, L.P.

```
  authentication attempt (default 60 seconds).

o 'server-timeout' sets the period of time after which the
  switch assumes that authentication has timed out
  (default 30 seconds).

o 'max-requests' sets the number of authentication attempts
  that must time out before authentication fails (default 3)

o 'max-retries' sets number of times a client can enter
  their credentials before authentication is considered
  to have failed (default 3).

o 'logoff-period' sets the period of time of inactivity that
  the switch considers an implicit logoff (default 300)

o 'reauth-period' sets the period of time after which connected
  clients must be re-authenticated.  When the timeout is set
  to 0 the re-authentication is disabled (default 0).

o 'auth-vid' configures the VLAN to which to move a port
  after successful authentication.  RADIUS server can
  override the value.  Use 'no' form of the command to set
  this PVID to 0.  If the PVID is set to 0 no PVID changes
  occur unless RADIUS server requests.  Changes take effect
  immediately.  All clients must immediately re-authenticate.
  The default is 0.

o 'unauth-vid' configures the VLAN to which to move a port
  after failed authentication.  Use 'no' form of the command
  to set this PVID to 0.  Changes take effect immediately.
  The default is 0.

o 'controlled-directions' configures how traffic is controlled
  on non-authenticated ports.
  - Both: (default)  In this mode, ingress+egress traffic
          to/from a non-authenticated port is controlled.
          For all practical purposes, only traffic related
          to the authentication process itself is allowed to
          pass through.
  - In:   In this mode, ingress traffic is controlled (in the
          same way as in 'both' mode; that is, only traffic
          related to authentication is allowed to pass).
          Traffic in the egress direction is not controlled
          by the authenticator.  This mode is very useful, for
          example, to a network administrator who wishes to
          deploy authentication and Wake-on-LAN.

          Note:  in order for a port to operationally be in the
                 'in' mode, this port must also be an edge port
                 ('spanning-tree <port> admin-edge-port');
                 this port's MAC must be functional (this port
                 must have link); and a BPDU must not be seen
                 on this port.

o 'reauthenticate' forces re-authentication
  of all clients present on a port.
```

Next Available Options:

- **web-list1** -- Manage web authentication based network authentication on the device port(s). ([ethernet] PORT-LIST) **(p. 52)**
- **dhcp-addr** -- Set the base address / mask for the temporary pool used by DHCP (base address default is 192.168.0.0, mask default is 24 - 255.255.255.0). (IP-ADDR/MASK-LENGTH) **(p. 30)**
- **dhcp-lease** < 5 to 25 > -- Set the lease length of the IP address issued by DHCP (default 10). (NUMBER) **(p. 30)**

web-list1

■ [no] aaa port-access web-based *[ETHERNET] PORT-LIST*

```
Manage web authentication based network authentication on the device port(s).
```

Next Available Options:

- **client-limit** < 1 to 32 > -- Set the port's maximum number of authenticated clients (default 1). (NUMBER) **(p. 28)**
- **client-moves** -- Set whether the client can move between ports (default disabled - no moves).**(p. 29)**
- **ssl-login** -- Set whether to enable SSL login (https on port 443) (default disabled).**(p. 45)**
- **redirect-url** -- Set the URL that the user should be redirected to after successful login (default none), Specify url up to 103 characters length.**(p. 43)**
- **max-retries** < 1 to 10 > -- Set number of times a client can enter their credentials before authentication is considered to have failed (default 3). (NUMBER) **(p. 36)**
- **logoff-period** < 1 to 9999999 > -- Set the period of time of inactivity that the switch considers an implicit logoff (default 300 seconds). (NUMBER) **(p. 33)**
- **quiet-period** < 1 to 65535 > -- Set the period of time the switch does not try to authenticate (default 60 seconds). (NUMBER) **(p. 42)**
- **server-timeout** < 1 to 300 > -- Set the authentication server response timeout (default 30 seconds). (NUMBER) **(p. 44)**
- **max-requests** < 1 to 10 > -- Set maximum number of times the switch retransmits authentication requests (default 3). (NUMBER) **(p. 35)**
- **reauth-period** < 0 to 9999999 > -- Set the re-authentication timeout in seconds; set to '0' to disable re-authentication (default 0). (NUMBER) **(p. 43)**
- **auth-vid** -- Configures VLAN where to move port after successful authentication (not configured by default).**(p. 28)**
- **unauth-vid** -- Configures VLAN where to keep port while there is an unauthorized client connected (not configured by default).**(p. 48)**
- **reauthenticate** -- Force re-authentication to happen.**(p. 43)**

web-redirect-url

■ aaa port-access web-based *[ETHERNET] PORT-LIST* redirect-url *WEB-REDIRECT-URL*

```
Set the URL that the user should be redirected to after successful login (default
none), Specify url up to 103 characters length.
```

web-unauthvid

■ aaa port-access web-based *[ETHERNET] PORT-LIST* unauth-vid *VLAN-ID*

```
Configures VLAN where to keep port while there is an unauthorized client connected
(not configured by default).
```

© 2007 Hewlett-Packard Development Company, L.P.

access-list

OVERVIEW

Category:	
Primary context:	config
Related Commands	**ip access-list**

```
Usage:
access-list <number> remark <remark>
access-list <CRF-NAME-STR> filter <ip | <ip-protocol> | <ip-protocol-nbr>>
                                  <ACL-IP-SPEC-SRC>
access-list <CRF-NAME-STR> ignore <ip | <ip-protocol> | <ip-protocol-nbr>>
                                  <ACL-IP-SPEC-SRC>
access-list <CRF-NAME-STR> filter <tcp | udp>  <ACL-IP-SPEC-SRC>
                                  destination-port <tcp-data>
                                  [source-port <tcp-data>]
access-list <CRF-NAME-STR> filter <tcp | udp>  <ACL-IP-SPEC-SRC>
                                  source-port <tcp-data>
                                  [destination-port <tcp-data>]
access-list <CRF-NAME-STR> ignore <tcp | udp>  <ACL-IP-SPEC-SRC>
                                  destination-port <tcp-data>
                                  [source-port <tcp-data>] [log]
access-list <CRF-NAME-STR> ignore <tcp | udp>  <ACL-IP-SPEC-SRC>
                                  source-port <tcp-data>
                                  [destination-port <tcp-data>] [log]
access-list <1-99> permit <ACL-IP-SPEC-SRC>
access-list <1-99> deny <ACL-IP-SPEC-SRC> [log]
access-list <100-199> permit <ip | <protocol>> <ACL-IP-SPEC-SRC>
                            <ACL-IP-SPEC-DST>
                            [precedence <precedence>] [tos <tos>]
access-list <100-199> deny <ip | <protocol>> <ACL-IP-SPEC-SRC>
                           <ACL-IP-SPEC-DST>
                           [precedence <precedence>] [tos <tos>] [log]
access-list <100-199> permit icmp <ACL-IP-SPEC-SRC> <ACL-IP-SPEC-DST>
                                  [<icmp-type> [<icmp-code>] | <icmp-message>]
                                  [precedence <precedence>] [tos <tos>] [log]
access-list <100-199> deny icmp <ACL-IP-SPEC-SRC> <ACL-IP-SPEC-DST>
                                  [<icmp-type> [<icmp-code>] | <icmp-message>]
                                  [precedence <precedence>] [tos <tos>] [log]
access-list <100-199> permit igmp <ACL-IP-SPEC-SRC> <ACL-IP-SPEC-DST>
                                   [<igmp-type>] [precedence <precedence>]
                                   [tos <tos>]
access-list <100-199> deny igmp <ACL-IP-SPEC-SRC> <ACL-IP-SPEC-DST>
                                  [<igmp-type>] [precedence <precedence>]
                                  [tos <tos>] [log]
access-list <100-199> permit tcp <ACL-IP-SPEC-SRC> [<ACL-PORT-SPEC-SRC>]
                                  <ACL-IP-SPEC-DST> [<ACL-PORT-SPEC-DST>]
                                  [established] [precedence <precedence>]
                                  [tos <tos>]
access-list <100-199> deny tcp <ACL-IP-SPEC-SRC> [<ACL-PORT-SPEC-SRC>]
                                 <ACL-IP-SPEC-DST> [<ACL-PORT-SPEC-DST>]
                                 [established] [precedence <precedence>]
                                 [tos <tos>] [log]
access-list <100-199> permit udp <ACL-IP-SPEC-SRC> [<ACL-PORT-SPEC-SRC>]
                                  <ACL-IP-SPEC-DST> [<ACL-PORT-SPEC-DST>]
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                                [precedence <precedence>] [tos <tos>]
access-list <100-199> deny udp <ACL-IP-SPEC-SRC> [<ACL-PORT-SPEC-SRC>]
                               <ACL-IP-SPEC-DST> [<ACL-PORT-SPEC-DST>]
                               [precedence <precedence>] [tos <tos>]
                               [log]
[no] access-list <number>

Description: Configure an entry in a standard (1-99) or extended (100-199)
             access control list.

Parameters:

    o <deny|permit> - specify action to take on a match.

    o <ACL-IP-SPEC> - specify the source or destination IP addresses to
      match.  The following formats may be used to specify IP addresses:
      * IP-ADDR MASK - match addresses defined by IP-ADDR using the bits
                       set to zero in MASK.
      * IP-ADDR/MASK-LEN - the mask is one in which the high order MASK-LEN
                           bits are zeros, and the remaining bits are ones.
                           172.16.0.0/18 translates to 172.16.0.0 0.0.63.255
      * host IP-ADDR - match a specific host; implies a mask of all zeros.
      * any          - match any IP address.

    o <filter | ignore> - specify action to take on a match.

    o log - log all matches.

    o <ip|tcp|udp> - specify protocol on which to match packets.

    o <ACL-PORT-SPEC> - for tcp or udp entries, specify the ports on which
      to match.  Port numbers may be specified as integers in the range
      1-65535, or by using protocol names for certain well-known ports.
      The following port specifications may be used:
      * eq <port>  - match packets from (to) the specified port.
      * neq <port> - match all packets except those from (to) the specified
                     port.
      * lt <port>  - match packets from (to) port numbers less than the
                     specified port.
      * gt <port>  - match packets from (to) port numbers greater than the
                     specified port.
      * range <port> <port> - match packets from (to) port numbers between
                     the first and second ports, inclusive.  The first port
                     specified must be less than the second port specified.

      The following well-known ports may be referred to by name:
      TCP: bgp, dns, ftp, http, imap4, ldap, nntp, pop2, pop3, smtp,
           ssl, telnet
      UDP: bootpc, bootps, dns, ntp, radius, radius-old, rip, snmp,
           snmp-trap, tftp

The following IP protocols may be referred to by name:

   o ip-in-ip     Match IP packets, as further specified.
   o ipv6-in-ip   Match IPv6 packets, as further specified.
   o gre          Match GRE packets, as further specified.
   o esp          Match ESP packets, as further specified.
   o ah           Match AH packets, as further specified.
   o ospf         Match OSPF packets, as further specified.
   o pim          Match PIM packets, as further specified.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
   o vrrp          Match VRRP packets, as further specified.
   o sctp          Match SCTP packets, as further specified.
   o icmp*         Match ICMP packets, as further specified.
   o igmp*         Match IGMP packets, as further specified.
   o ip            Match all IP packets.
   o tcp           Match TCP packets, as further specified.
   o udp           Match UDP packets, as further specified.

* These IP protocols may not be used with connection-rate-filter ACLs.

The following ICMP packet-types may be referred to by name:

   o administratively-prohibited
   o alternate-address conversion-error
   o dod-host-prohibited
   o dod-net-prohibitedecho
   o echo-reply
   o general-parameter-problem
   o host-isolated
   o host-precedence-unreachable
   o host-redirect
   o host-tos-redirect
   o host-tos-unreachable
   o host-unknown
   o host-unreachable
   o information-reply
   o information-request
   o mask-reply
   o mask-request
   o mobile-redirect
   o net-redirect
   o net-tos-redirect
   o net-tos-unreachable

IGMP packet-type options

   o dvmrp
   o host-query
   o host-report
   o pim
   o trace
   o v2-host-report
   o v2-host-leave
   o mtrace-reply
   o mtrace-request
   o v3-host-report


For more information on Connection-Rate ACLs, see Chapter 3 "Virus Throttling"
in the Access Security Guide [http://www.hp.com/rnd/support/manuals/5400zl.htm] for the
 Series 5400zl, Series 3500yl, and 6200yl Switches.

For more information on ACLs, see Chapter 10 "Access Control Lists (ACLs)" in the
Access Security Guide [http://www.hp.com/rnd/support/manuals/5400zl.htm] for the Series
 5400zl, Series 3500yl, and 6200yl Switches.
```

© 2007 Hewlett-Packard Development Company, L.P.

arp-protect

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] arp-protect [trust [ethernet] PORT-LIST|
                        validate <ip|destination-mac|src-mac>|
                        vlan VLAN-ID-RANGE]

Description: Configure Dynamic ARP Protection.
             To Enable/disable ARP Protection on the switch execute the
             [no] arp-protect command. Dynamic ARP Protection will not be
             enabled on any VLAN if it is not enabled on the switch.
             By default Dynamic ARP Protection is disabled.
             To configure which VLANs are to be protected execute the
             'arp-protect vlan' command. By default Dynamic ARP Protection
             is disabled on all VLANs.

             Dynamic ARP Protection divides ports into two categories:
             untrusted and trusted. ARP packets received on trusted ports
             are forwarded without validation.
             ARP packets received on the untrusted ports of a protected VLAN
             are intercepted and validated before being forwarded.
             By default ports are untrusted.

             Dynamic ARP Protection validates ARP packets based on the
             IP-to-MAC binding database maintained by DHCP snooping. If DHCP
             snooping is not enabled then a loss of connectivity will result
             since the database will contain no bindings. For devices that do
             not use DHCP to obtain their IP configuration static bindings can
             be added manually to the database with the 'ip source-binding'
             command.

             Dynamic ARP Protection can also be configured to drop ARP packets
             that contain invalid IP addresses or when the MAC addresses in the
             body of the ARP packet do not match those in the ethernet header.

Parameters:
      trust [ethernet] PORT-LIST     -- Configure ports as trusted or untrusted.
      validate <ip|dest-mac|src-mac> -- Configure addiional ARP packet checks.
      vlan VLAN-ID-RANGE             -- Enable/disable ARP Protection on VLANs
```

COMMAND STRUCTURE

- [no] arp-protect **trust** -- Configure port(s) as trusted or untrusted. ([ethernet] PORT-LIST) **(p. 57)**
- [no] arp-protect **validate** -- Configure additional ARP Protection validation checks. **(p. 57)**
  - **dest-mac** -- Drop any ARP response packet in which the destination MAC address in the ethernet header does not match the target MAC address in the body of the packet. **(p. 57)**
  - **ip** -- Drop any ARP request with an invalid sender IP address. Drop any ARP response with an invalid target IP address. Invalid IP addresses include 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all class E IP addresses. **(p. 57)**

© 2007 Hewlett-Packard Development Company, L.P.

- **src-mac** -- Drop any ARP request or response packet in which the source MAC in the ethernet header does not match the sender MAC address in the body of the packet. **(p. 57)**

■ [no] arp-protect **vlan** -- Enable/disable Dynamic ARP Protection on a VLAN(s). **(p. 58)**

- **vlan-list** -- (VLAN-ID-RANGE) **(p. 58)**

COMMAND DETAILS

dest-mac (p. 57)	**trust (p. 57)**	**vlan-list (p. 58)**
ip (p. 57)	**validate (p. 57)**	
src-mac (p. 57)	**vlan (p. 58)**	

dest-mac

■ [no] arp-protect validate dest-mac

```
Drop any ARP response packet in which the destination MAC address in the
ethernet header does not match the target MAC address in the body of the
packet.
```

ip

■ [no] arp-protect validate ip

```
Drop any ARP request with an invalid sender IP address. Drop any ARP
response with an invalid target IP address. Invalid IP addresses include
0.0.0.0, 255.255.255.255, all IP multicast addresses, and all class E
IP addresses.
```

src-mac

■ [no] arp-protect validate src-mac

```
Drop any ARP request or response packet in which the source MAC in the
ethernet header does not match the sender MAC address in the body of
the packet.
```

trust

■ [no] arp-protect trust *[ETHERNET] PORT-LIST*

```
Configure port(s) as trusted or untrusted.
```

validate

■ [no] arp-protect validate

```
Configure additional ARP Protection validation checks.
```

Next Available Options:

- **src-mac** -- Drop any ARP request or response packet in which the source MAC in the ethernet header does not match the sender MAC address in the body of the packet. **(p. 57)**
- **dest-mac** -- Drop any ARP response packet in which the destination MAC address in the ethernet header does not match the target MAC address in the body of the packet. **(p. 57)**
- **ip** -- Drop any ARP request with an invalid sender IP address. Drop any ARP response with an invalid target IP address. Invalid IP addresses include 0.0.0.0, 255.255.255.255, all IP multicast addresses, and all class E IP addresses. **(p. 57)**

© 2007 Hewlett-Packard Development Company, L.P.

vlan

- [no] arp-protect vlan

  ```
  Enable/disable Dynamic ARP Protection on a VLAN(s).
  ```

  Next Available Option:
  - **vlan-list** -- (VLAN-ID-RANGE) **(p. 58)**

vlan-list

- [no] arp-protect vlan *VLAN-ID-RANGE*

© 2007 Hewlett-Packard Development Company, L.P.

auto-tftp

OVERVIEW

Category:	File Transfer
Primary context:	config
Related Commands	tftp (page 443)

```
Usage: [no] auto-tftp [IP-ADDR FILENAME-STR]

Description: Enable/disable automatic OS image download via TFTP during
             boot. The OS image will be downloaded if it has a different
             version from the OS running on the switch. The command requires
             the parameters to be specified when used without 'no'.
             If auto-tftp is configured on the switch, the 'no' form of this
             command deletes the auto-tftp entry from the switch configuration,
             thus preventing auto-tftp operation if the switch reboots.
             Note: This command does not affect the current TFTP-enable
                   configuration on the switch.
             o IP-ADDR - specifies the TFTP server IP address to download
               an OS image from.
             o FILENAME-STR - specifies the file-name to download.
```

COMMAND STRUCTURE

- auto-tftp **server-ip** -- IP address of the TFTP server to download an OS image from. (IP-ADDR) **(p. 59)**
  - **filename** -- The OS image file-name. (ASCII-STR) **(p. 59)**

EXAMPLES

Example: auto-tftp IP-ADDR FILENAME

Set the device to boot using image2 located on TFTP server 10.10.2.40, if the image version is different from the one already on the switch:

```
ProCurve(config)# auto-tftp 10.10.2.40 image2
```

COMMAND DETAILS

filename (p. 59)	**server-ip (p. 59)**

filename

- auto-tftp *IP-ADDR FILENAME*

```
The OS image file-name.
```

server-ip

- auto-tftp *IP-ADDR*

```
IP address of the TFTP server to download an OS image from.
```

Next Available Option:

- **filename** -- The OS image file-name. (ASCII-STR) **(p. 59)**

© 2007 Hewlett-Packard Development Company, L.P.

banner

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show banner (page 337)**

```
Usage: [no] banner motd ASCII-STR

Description: Define a login banner. The banner will be displayed before
             login on the console, telnet, ssh, and Web-UI sessions.
             The banner can be a multi-line text up to 320 characters.
             The banner text can contain any printable character except
             the delimiting character and the ~ character.
```

COMMAND STRUCTURE

- [no] banner **motd** -- Set message of the day banner **(p. 60)**
  - **ascii** -- Specify delimiting character for banner text (ASCII-STR) **(p. 60)**

EXAMPLES

Example: banner motd DELIMITER

Configure a banner message that reads "Welcome to this ProCurve switch." and verify it:

```
ProCurve(config)# banner motd >
Enter TEXT message. End with the character'>'
Welcome to this ProCurve switch.>

ProCurve(config)# show banner motd
Banner Information Banner status: Enabled
Configured Banner:
Welcome to this ProCurve switch.
```

COMMAND DETAILS

ascii (p. 60)	**motd (p. 60)**

ascii

- banner motd *ASCII*

```
Specify delimiting character for banner text
```

motd

- [no] banner motd

```
Set message of the day banner
```

Next Available Option:
- **ascii** -- Specify delimiting character for banner text (ASCII-STR) **(p. 60)**

© 2007 Hewlett-Packard Development Company, L.P.

boot

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	reload (page 288)

```
Usage: boot [system [flash <primary|secondary>] [config FILENAME]]

Description: Reboot the device. The primary or secondary software image
             can be specified to be used during the boot process.
             Optionally, a configuration file can be set for this boot.
```

COMMAND STRUCTURE

- boot **system** -- Allows to specify boot image to use after reboot. (p. 62)
  - **flash < primary | secondary >** -- Specify boot image to use after reboot. (p. 62)
    - **config < config1 >** -- Specify configuration file to use on boot. (p. 61)

EXAMPLES

Example: boot

Boot the switch from primary flash with pending configuration changes in the running-config file:

```
HPswitch(config)# boot

Device will be rebooted, do you want to continue [y/n]?  y
Boot from primary flash

Do you want to save current configuration [y/n]?
```

Example: boot system flash secondary

Reboot the switch from secondary flash when there are no pending configuration changes in the running-config file:

```
HPswitch(config)# boot system flash secondary

Device will be rebooted, do you want to continue [y/n]?  y
Boot from secondary flash

Do you want to save current configuration [y/n]?
```

COMMAND DETAILS

config (p. 61)	flash (p. 62)	system (p. 62)

config

- boot system flash *< primary | secondary >* config *< config1>*

  ```
  Specify configuration file to use on boot.
  ```

  Supported Values:

© 2007 Hewlett-Packard Development Company, L.P.

- **config1**

flash

- boot system flash *< primary | secondary >*

```
Specify boot image to use after reboot.
```

Supported Values:
- **primary** -- Primary flash image.
- **secondary** -- Secondary flash image.

Next Available Option:
- **config** < config1 > -- Specify configuration file to use on boot.**(p. 61)**

system

- boot system

```
Allows to specify boot image to use after reboot.
```

Next Available Option:
- **flash** < primary | secondary > -- Specify boot image to use after reboot.**(p. 62)**

© 2007 Hewlett-Packard Development Company, L.P.

cdp

OVERVIEW

Category:	Routing
Primary context:	config
Related Commands	**show cdp (page 339)**

```
Usage: [no] cdp ...

Description: Set various CDP (Cisco Discovery Protocol) parameters. Use
             'cdp ?' to get a list of all possible options.
```

COMMAND STRUCTURE

- [no] cdp **enable** -- Enable/disable CDP on particular device ports ([ethernet] PORT-LIST) **(p. 63)**
- [no] cdp **run** -- Start and stop CDP on the device **(p. 63)**

EXAMPLES

Example: cdp enable PORT-LIST

Disable CDP on port A1 of a Series 5400zl switch:

```
ProCurve(config)# no cdp enable a1
```

Example: cdp run

Disable CDP on the switch:

```
ProCurve(config)# no cdp run
```

COMMAND DETAILS

enable (p. 63)	**run (p. 63)**

enable

- [no] cdp enable *[ETHERNET] PORT-LIST*

```
Usage: [no] cdp enable [ethernet] PORT-LIST

Description: Enable/disable CDP on particular device ports.
```

run

- [no] cdp run

```
Usage: [no] cdp run

Description: Start and stop CDP on the device.
```

© 2007 Hewlett-Packard Development Company, L.P.

chassislocate

OVERVIEW

Category:	
Primary context:	operator
Related Commands	

```
Usage: chassislocate <on|blink> [<1-1440>]
       chassislocate off

Description: Control the chassis locate led.

Parameters:

    o on - Turn the led on.
    o off - Turn the led off.
    o blink - Make the led blink.
    o [<1-1440>] - Number of minutes the led is
                   to blink or be turned on (default is 30).
```

COMMAND STRUCTURE

- chassislocate **blink** -- Blink the chassis locate led (default 30 minutes). **(p. 64)**
  - **duration < 1 to 1440 >** -- Number of minutes duration (default 30). (NUMBER) **(p. 64)**
- chassislocate **off** -- Turn the chassis locate led off. **(p. 65)**
- chassislocate **on** -- Turn the chassis locate led on (default 30 minutes). **(p. 65)**
  - **duration < 1 to 1440 >** -- Number of minutes duration (default 30). (NUMBER) **(p. 64)**

COMMAND DETAILS

blink (p. 64)	**off (p. 65)**
duration (p. 64)	**on (p. 65)**

blink

- chassislocate blink

```
Blink the chassis locate led (default 30 minutes).
```

Next Available Option:
- **duration** < 1 to 1440 > -- Number of minutes duration (default 30). (NUMBER) **(p. 64)**

duration

- chassislocate on *< 1 to 1440 >*

```
Number of minutes duration (default 30).
```

Range: < 1 to 1440 >
- chassislocate blink *< 1 to 1440 >*

```
Number of minutes duration (default 30).
```

Range: < 1 to 1440 >

© 2007 Hewlett-Packard Development Company, L.P.

off

- chassislocate off

```
Turn the chassis locate led off.
```

on

- chassislocate on

```
Turn the chassis locate led on (default 30 minutes).
```

Next Available Option:

- **duration** < 1 to 1440 > -- Number of minutes duration (default 30). (NUMBER) **(p. 64)**

© 2007 Hewlett-Packard Development Company, L.P.

clear

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: clear <arp|intrusion-log|logging|public-key|statistics
              [ethernet] PORT-LIST |link-keepalive statistics>

Description: Clear table/statistics or authorized client public keys.

Parameters:

    o arp - Flushes all non-permanent entries in the ARP cache.

    o intrusion-log - Resets the Alert Flags and prepares
      the switch to detect and log the next security intrusion.

    o logging - Remove all event entries from the event log

    o public-key - Removes currently loaded authorized client public keys
      from active configuration.

    o statistics PORT-LIST - Resets all port counters associated with
      the ports specified.

    o link-keepalive statistics - Resets the UDLD packets sent, UDLD
      packets received, and Transition counters for all UDLD enabled ports.
```

COMMAND STRUCTURE

- clear **arp** -- Flush all non-permanent entries in the ARP cache. **(p. 67)**
- clear **crypto** -- Remove client public keys from active configuration. **(p. 67)**
  - **client-public-key** -- Remove client public keys from active configuration. **(p. 67)**
    - **keyfile < manager | operator >** -- Remove client public keys from active configuration. **(p. 67)**
      - **keylist** -- Remove client public keys from active configuration. (ASCII-STR) **(p. 67)**
- clear **intrusion-flags** -- Reset the Alert Flag on all ports. **(p. 67)**
- clear **link-keepalive** -- Reset link-keepalive counters for all UDLD enabled ports. **(p. 67)**
  - **statistics** -- Reset link-keepalive counters for all UDLD enabled ports. **(p. 68)**
- clear **link-keepalive** -- Reset link-keepalive counters for all UDLD enabled ports. **(p. 67)**
  - **statistics** -- Reset link-keepalive counters for all UDLD enabled ports. **(p. 68)**
- clear **logging** -- Remove all event entries from the event log. **(p. 68)**
- clear **statistics** -- Reset all counters for the specified ports. ([ethernet] PORT-LIST) **(p. 68)**

COMMAND DETAILS

arp (p. 67)	**intrusion-flags (p. 67)**	**link-keepalive (p. 67)**
client-public-key (p. 67)	**keyfile (p. 67)**	**logging (p. 68)**
crypto (p. 67)	**keylist (p. 67)**	**statistics (p. 68)**

© 2007 Hewlett-Packard Development Company, L.P.

arp

- clear arp

```
Flush all non-permanent entries in the ARP cache.
```

client-public-key

- clear crypto client-public-key

```
Remove client public keys from active configuration.
```

Next Available Option:

- **keyfile** < manager | operator > -- Remove client public keys from active configuration.**(p. 67)**

crypto

- clear crypto

```
Remove client public keys from active configuration.
```

Next Available Option:

- **client-public-key** -- Remove client public keys from active configuration.**(p. 67)**

intrusion-flags

- clear intrusion-flags

```
Reset the Alert Flag on all ports.
```

keyfile

- clear crypto client-public-key *< manager | operator >*

```
Remove client public keys from active configuration.
```

Supported Values:

- **manager** -- Select manager public keys.
- **operator** -- Select operator public keys.

Next Available Option:

- **keylist** -- Remove client public keys from active configuration. (ASCII-STR) **(p. 67)**

keylist

- clear crypto client-public-key *< manager | operator > KEYLIST*

```
Remove client public keys from active configuration.
```

link-keepalive

- clear link-keepalive

```
Reset link-keepalive counters for all UDLD enabled ports.
```

Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **statistics** -- Reset link-keepalive counters for all UDLD enabled ports.**(p. 68)**

logging

- clear logging

  ```
  Remove all event entries from the event log.
  ```

statistics

- clear statistics *[ETHERNET] PORT-LIST*

  ```
  Reset all counters for the specified ports.
  ```

- clear link-keepalive statistics

  ```
  Reset link-keepalive counters for all UDLD enabled ports.
  ```

© 2007 Hewlett-Packard Development Company, L.P.

clock

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	ip (page 180) sntp (page 413) time (page 444)

```
Usage: [no] clock [...]

Description: Display/set current time, date, and local time parameters.
             Called without any parameters displays the information
             mentioned above. Use 'clock ?' to see a list of all possible
             configuration options.
```

NOTES

When to Use this Command

Use this command to set the time and date only if the switch will not use TimeP or SNTP to learn the time and date from a time server.

COMMAND STRUCTURE

- clock **set** -- Set current time and/or date **(p. 70)**
  - **date** -- Current date to set. (MM/DD[/[YY]YY]) **(p. 69)**
  - **time** -- Current time to set. (HH:MM[:SS]) **(p. 71)**
- [no] clock **summer-time** -- Enable/disable daylight-saving time changes **(p. 70)**
- clock **timezone** -- Set the number of hours your location is to the West(-) or East(+) of GMT **(p. 71)**
  - **gmt < +14:00 | +13:00 | +12:00 | ... >** -- Number of hours your timezone is to the West(-) or East(+) of GMT. **(p. 69)**
  - **us < alaska | aleutian | arizona | ... >** -- Timezone for US locations. **(p. 71)**

COMMAND DETAILS

date (p. 69)	**summer-time (p. 70)**	**us (p. 71)**
gmt (p. 69)	**time (p. 71)**	
set (p. 70)	**timezone (p. 71)**	

date

- clock set *[DATE]*

```
Current date to set.
```

gmt

- clock timezone gmt *< +14:00 | +13:00 | +12:00 | ... >*

```
Number of hours your timezone is to the West(-) or East(+) of GMT.
```

Supported Values:

- **+14:00**

© 2007 Hewlett-Packard Development Company, L.P.

- **+13:00**
- **+12:00**
- **+11:30**
- **+11:00**
- **+10:30**
- **+10:00**
- **+9:30**
- **+9:00**
- **+8:00**
- **+7:00**
- **+6:30**
- **+6:00**
- **+5:30**
- **+5:00**
- **+4:30**
- **+4:00**
- **+3:30**
- **+3:00**
- **+2:00**
- **+1:00**
- **+0:00**
- **-1:00**
- **-2:00**
- **-3:00**
- **-3:30**
- **-4:00**
- **-5:00**
- **-6:00**
- **-7:00**
- **-8:00**
- **-8:30**
- **-9:00**
- **-9:30**
- **-10:00**
- **-11:00**
- **-12:00**

set

- clock set

```
Usage: clock set <[MM/DD[/[YY]YY]] [HH:MM[:SS]]>

Description: Set current time and/or date.
             o MM/DD[/[YY]YY]   - New date
             o HH:MM[:SS]       - New time
```

Next Available Options:

- **date** -- Current date to set. (MM/DD[/[YY]YY]) **(p. 69)**
- **time** -- Current time to set. (HH:MM[:SS]) **(p. 71)**

summer-time

- [no] clock summer-time

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] clock summer-time

Description: Enable/disable daylight-saving time changes.
```

time

- clock set *[TIME]*

```
Current time to set.
```

timezone

- clock timezone

```
Usage: clock timezone [gmt <-12:00 - +14:00>] |
                      [us  <none|alaska|aleutian|arizona|central|
                            east-indiana|eastern|hawaii|michigan|mountain|
                            pacific|samoa>]

Description: Set the number of hours your location is to the
             West(-) or East(+) of GMT. The number of hours can
             be defined by specifying either an exact number
             (see 'clock timezone gmt ?' for the list of all acceptable
             values) or a US timezone. The default value is GMT 0.
```

Next Available Options:

- **gmt** < +14:00 | +13:00 | +12:00 | ... > -- Number of hours your timezone is to the West(-) or East(+) of GMT.**(p. 69)**
- **us** < alaska | aleutian | arizona | ... > -- Timezone for US locations.**(p. 71)**

us

- clock timezone us *< alaska | aleutian | arizona | ... >*

```
Timezone for US locations.
```

Supported Values:

- **alaska**
- **aleutian**
- **arizona**
- **central**
- **east_indiana**
- **eastern**
- **hawaii**
- **michigan**
- **mountain**
- **pacific**
- **samoa**

© 2007 Hewlett-Packard Development Company, L.P.

configure

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**end (page 135)** **exit (page 138)** **enable (page 134)**

```
Usage: configure [terminal]

Description: Enter the Configuration context.
```

COMMAND STRUCTURE

- configure **terminal** -- Optional keyword of the configure command, could be omitted. **(p. 72)**

EXAMPLES

Example: enable

```
ProCurve# configure
ProCurve(config)#
```

COMMAND DETAILS

terminal (p. 72)

terminal

- configure terminal

```
Optional keyword of the configure command, could be omitted.
```

© 2007 Hewlett-Packard Development Company, L.P.

connection-rate-filter

OVERVIEW

Category:	Troubleshooting
Primary context:	config
Related Commands	**filter (page 142)** **ip (page 180)** **vlan (page 457)** **show connection-rate-filter (page 344)**

```
Usage:      connection-rate-filter unblock < host SRC-IP-ADDR | SRC-IP-ADDRESS/MASK >
       [no] connection-rate-filter sensitivity <low|medium|high|aggressive>

Description: Globally enable connection rate filtering and set the sensitivity, or
             stop blocking traffic from hosts already being blocked by connection
             rate filtering.
             To put connection rate filtering into effect, you also must configure
             it on individual ports, in addition to globally enabling the feature.
             Use the "connection-rate-filter <...>" command in the Interface
             context.
```

COMMAND STRUCTURE

- connection-rate-filter **sensitivity** -- Sets the level of filtering required **(p. 74)**
  - **sensitive < low | medium | high | ... >** -- **(p. 73)**
- connection-rate-filter **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 74)**
  - **all** -- Resets all previously blocked by the connection rate filter **(p. 73)**
  - **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 73)**
  - **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 74)**

COMMAND DETAILS

all (p. 73)	**sensitive (p. 73)**	**src-ip (p. 74)**
host (p. 73)	**sensitivity (p. 74)**	**unblock (p. 74)**

all

- connection-rate-filter unblock all

```
Resets all previously blocked by the connection rate filter
```

host

- connection-rate-filter unblock host *IP-ADDR*

```
Match packets from the specified IP address.
```

sensitive

- connection-rate-filter sensitivity *< low | medium | high | ... >*

  Supported Values:
  - **low** -- Sets the level of connection rate filtering to low (most permissive)

© 2007 Hewlett-Packard Development Company, L.P.

- **medium** -- Sets the level of connection rate filtering to medium (permissive)
- **high** -- Sets the level of connection rate filtering to high (restrictive)
- **aggressive** -- Sets the level of connection rate filtering to aggressive (most restrictive)

sensitivity

- connection-rate-filter sensitivity

```
Sets the level of filtering required
```

Next Available Option:

- **sensitive** < low | medium | high | ... > -- **(p. 73)**

src-ip

- connection-rate-filter unblock *IP-ADDR/MASK-LENGTH*

```
Match packets from the specified subnet.
```

unblock

- connection-rate-filter unblock

```
Resets a host previously blocked by the connection rate filter
```

Next Available Options:

- **all** -- Resets all previously blocked by the connection rate filter **(p. 73)**
- **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 73)**
- **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 74)**

© 2007 Hewlett-Packard Development Company, L.P.

console

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show console (page 344)** **repeat (page 291)**

```
Usage: console ...

Description: Set various console parameters. Use 'console ?' to get a list
             of all configurable parameters.
             The non-configurable parameters and their default values are:
             Data bits = 8; Parity = None; Stop bits = 1.
```

COMMAND STRUCTURE

- console **baud-rate < speed-sense | 1200 | 2400 | ... >** -- Set the data transmission speed for the device connect sessions initiated through the Console port **(p. 76)**
- console **events < None | Debug | All | ... >** -- Set level of the events displayed in the device's Events Log **(p. 76)**
- console **flow-control < XON/XOFF | None >** -- Set the Flow Control Method; default is xon-xoff **(p. 76)**
- console **inactivity-timer < 0 | 1 | 5 | ... >** -- Set the number of minutes of no activity detected on the Console port before the switch terminates a communication session **(p. 77)**
- console **local-terminal < VT100 | NONE | ANSI >** -- Set type of terminal being used for the current console or telnet session (default is vt100) **(p. 77)**
- console **screen-refresh < 1 | 3 | 5 | ... >** -- Set default number of seconds before screen is refreshed on the repeat command **(p. 77)**
- console **terminal < VT100 | NONE | ANSI >** -- Set type of terminal being used for all console and telnet sessions (default is vt100) **(p. 78)**

EXAMPLES

Example: console <...>

Configure the switch to use the following console settings:

- VT100 operation
- 19,200 baud
- No flow control
- 10-minute inactivity time
- Critical log events

© 2007 Hewlett-Packard Development Company, L.P.

```
HPswitch(config)# console terminal vt100 baud-rate 19200 flow-control none
inactivity-timer 10 events critical
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# reload
```

COMMAND DETAILS

baud-rate (p. 76)	inactivity-timer (p. 77)	terminal (p. 78)
events (p. 76)	local-terminal (p. 77)	
flow-control (p. 76)	screen-refresh (p. 77)	

baud-rate

- console baud-rate *< speed-sense | 1200 | 2400 | ... >*

```
Usage: console baud-rate <speed-sense|1200|2400|4800|
                          9600|19200|38400|57600|115200>

Description: Set the data transmission speed for the device connect
             sessions initiated through the Console port. The 'speed-sense'
             is for automatic speed determination. Default is speed-sense.
```

Supported Values:

- **speed-sense**
- **1200**
- **2400**
- **4800**
- **9600**
- **19200**
- **38400**
- **57600**
- **115200**

events

- console events *< None | Debug | All | ... >*

```
Usage: console events <none|all|not-info|critical|debug>

Description: Set level of the events displayed in the device's Events Log.
             all - display all;
             none - display no events;
             not-info - display all events except informational;
             critical - display only critical-level events;
             debug - reserved for Internal use.
```

Supported Values:

- **None**
- **Debug**
- **All**
- **Not-INFO**
- **Critical**

flow-control

- console flow-control *< XON/XOFF | None >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: console flow-control <xon/xoff|none>

Description: Set the Flow Control Method; default is xon-xoff.
```

Supported Values:
- **XON/XOFF**
- **None**

inactivity-timer

- console inactivity-timer *< 0 | 1 | 5 | ... >*

```
Usage: console inactivity-timer <0|1|5|10|15|20|30|60|120>

Description: Set the number of minutes of no activity detected on the
             Console port before the switch terminates a communication
             session. '0' means disable inactivity timer.
             Default is 0.
```

Supported Values:
- **0**
- **1**
- **5**
- **10**
- **15**
- **20**
- **30**
- **60**
- **120**

local-terminal

- console local-terminal *< VT100 | NONE | ANSI >*

```
Usage: console local-terminal <vt100|ansi|none>

Description: Set type of terminal being used for the current
             console or telnet session (default is vt100).
             Takes effect immediately. Not saved in configuration.

             Terminal type options are:
             vt100 = use VT100 terminal escape sequences.
             ansi = use ANSI terminal escape sequences.
             none = use a raw mode with no terminal escape sequences. Useful
             for scripting.

             See also 'console terminal help'.
```

Supported Values:
- **VT100** -- VT-100 terminal compatible.
- **NONE** -- Raw mode with terminal escape sequences removed.
- **ANSI** -- ANSI terminal compatible.

screen-refresh

- console screen-refresh *< 1 | 3 | 5 | ... >*

```
Usage: console screen-refresh <1|3|5|10|20|30|45|60>

Description: Set default number of seconds before screen is refreshed
```

© 2007 Hewlett-Packard Development Company, L.P.

```
              on the repeat command. See 'repeat help' for details on
              the 'repeat' command.
```

Supported Values:

- **1**
- **3**
- **5**
- **10**
- **20**
- **30**
- **45**
- **60**

terminal

- console terminal *< VT100 | NONE | ANSI >*

```
Usage: console terminal <vt100|ansi|none>

Description: Set type of terminal being used for all console
             and telnet sessions (default is vt100).  Saved in
             configuration and requires reboot to take effect.

             Terminal type options are:
             vt100 = use VT100 terminal escape sequences.
             ansi = use ANSI terminal escape sequences.
             none = use a raw mode with no terminal escape sequences. Useful
             for scripting.

             See also 'console local-terminal help'.
```

Supported Values:

- **VT100** -- VT-100 terminal compatible.
- **NONE** -- Raw mode with terminal escape sequences removed.
- **ANSI** -- ANSI terminal compatible.

© 2007 Hewlett-Packard Development Company, L.P.

copy

OVERVIEW

Category:	File Transfer
Primary context:	manager
Related Commands	**show config (page 341)** **show flash (page 350)** **show running-config (page 378)**

```
Usage: copy <source> <destination> [options]

Description: Copy datafiles to/from the switch.

   <source> - specify source of data. It can be 'tftp', 'xmodem', 'command',
              'usb' or any of the following switch data files:
              o running-config
              o startup-config
              o crash-log [a|b|c|d|e|f|g|h|master]
              o crash-data
              o event-log
              o command-output <command>

          Note: When using 'command-output', place the desired CLI command in
                double-quotes. i.e. "show system".

   <destination> - specify the copy target. It can be also 'tftp', 'xmodem',
             'usb' or one of the following switch data files:
              o startup-config
              o command-file
              o flash
              o pub-key-file

   [options] - options are:
              o IP address - TFTP server address.
                             Required for TFTP transfers.
              o filename   - File-name to upload/download.
                             Required for TFTP & USB transfers.
              o unix
              o pc
```

COMMAND STRUCTURE

- copy **command-output** -- Specify a CLI command to copy output of. (ASCII-STR) **(p. 84)**
  - **tftp** -- Copy data to a TFTP server. **(p. 97)**
    - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
        - **pc** -- Change CR/LF to PC style. **(p. 92)**
        - **unix** -- Change CR/LF to unix style. **(p. 101)**
  - **usb** -- Copy data to a USB flash drive. **(p. 102)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
    - **pc** -- Change CR/LF to PC style. **(p. 92)**
    - **unix** -- Change CR/LF to unix style. **(p. 101)**
- copy **config < config1 >** -- Copy named configuration file. **(p. 84)**

© 2007 Hewlett-Packard Development Company, L.P.

- **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 84)**
- **tftp** -- Copy data to a TFTP server. **(p. 97)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
      - **pc** -- Change CR/LF to PC style. **(p. 92)**
      - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
  - **pc** -- Change CR/LF to PC style. **(p. 92)**
  - **unix** -- Change CR/LF to unix style. **(p. 101)**

■ copy **crash-data** -- Copy the switch crash data file. **(p. 85)**
- **card** -- Enter single slot identifier. (SLOT-ID-RANGE) **(p. 83)**
  - **tftp** -- Copy data to a TFTP server. **(p. 97)**
    - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
  - **usb** -- Copy data to a USB flash drive. **(p. 102)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
- **master** -- Copy from the master card (default). **(p. 91)**
  - **tftp** -- Copy data to a TFTP server. **(p. 97)**
    - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
  - **usb** -- Copy data to a USB flash drive. **(p. 102)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
- **tftp** -- Copy data to a TFTP server. **(p. 97)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
- **usb** -- Copy data to a USB flash drive. **(p. 102)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
- **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**

■ copy **crash-log** -- Copy the switch log file. **(p. 85)**
- **card** -- Enter single slot identifier. (SLOT-ID-RANGE) **(p. 83)**
  - **tftp** -- Copy data to a TFTP server. **(p. 97)**
    - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
  - **usb** -- Copy data to a USB flash drive. **(p. 102)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
- **master** -- Copy from the master card (default). **(p. 91)**
  - **tftp** -- Copy data to a TFTP server. **(p. 97)**
    - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
      - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
  - **usb** -- Copy data to a USB flash drive. **(p. 102)**
    - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
  - **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
- **tftp** -- Copy data to a TFTP server. **(p. 97)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
- **usb** -- Copy data to a USB flash drive. **(p. 102)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
- **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**

■ copy **event-log** -- Copy event log file. **(p. 86)**

© 2007 Hewlett-Packard Development Company, L.P.

- **tftp** -- Copy data to a TFTP server. **(p. 97)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
      - **pc** -- Change CR/LF to PC style. **(p. 92)**
      - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **usb** -- Copy data to a USB flash drive. **(p. 102)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
- **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
  - **pc** -- Change CR/LF to PC style. **(p. 92)**
  - **unix** -- Change CR/LF to unix style. **(p. 101)**

■ copy **flash** -- Copy the switch system image file. **(p. 90)**
- **flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 90)**
- **tftp** -- Copy data to a TFTP server. **(p. 97)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
- **usb** -- Copy data to a USB flash drive. **(p. 102)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
- **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**

■ copy **running-config** -- Copy running configuration file. **(p. 93)**
- **tftp** -- Copy data to a TFTP server. **(p. 97)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
      - **pc** -- Change CR/LF to PC style. **(p. 92)**
      - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **usb** -- Copy data to a USB flash drive. **(p. 102)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
- **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
  - **pc** -- Change CR/LF to PC style. **(p. 92)**
  - **unix** -- Change CR/LF to unix style. **(p. 101)**

■ copy **startup-config** -- Copy in-flash configuration file. **(p. 93)**
- **tftp** -- Copy data to a TFTP server. **(p. 97)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
      - **pc** -- Change CR/LF to PC style. **(p. 92)**
      - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **usb** -- Copy data to a USB flash drive. **(p. 102)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
- **xmodem** -- Use xmodem on the terminal as the data destination. **(p. 104)**
  - **pc** -- Change CR/LF to PC style. **(p. 92)**
  - **unix** -- Change CR/LF to unix style. **(p. 101)**

■ copy **tftp** -- Copy data from a TFTP server. **(p. 97)**
- **command-file** -- Copy command script to switch and execute. **(p. 84)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
      - **pc** -- Change CR/LF to PC style. **(p. 92)**
      - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 84)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
      - **pc** -- Change CR/LF to PC style. **(p. 92)**
      - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **flash** -- Copy data to the switch system image file. **(p. 90)**

© 2007 Hewlett-Packard Development Company, L.P.

- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
    - **cv_flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 86)**
- **pub-key-file** -- Copy the public keys to the switch. **(p. 93)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
      - **append** -- Add the key(s) for operator access. **(p. 83)**
      - **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s). **(p. 91)**
        - **append** -- Add the key(s) for access. **(p. 83)**
      - **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s). **(p. 92)**
        - **append** -- Add the key(s) for access. **(p. 83)**
- **startup-config** -- Copy data to the switch configuration file. **(p. 93)**
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**
    - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**
      - **pc** -- Change CR/LF to PC style. **(p. 92)**
      - **unix** -- Change CR/LF to unix style. **(p. 101)**

■ copy **usb** -- Copy data from a USB flash drive. **(p. 102)**

- **command-file** -- Copy command script to switch and execute. **(p. 84)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
    - **pc** -- Change CR/LF to PC style. **(p. 92)**
    - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **flash** -- Copy data to the switch system image file. **(p. 90)**
  - **image-name** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 91)**
    - **cv_flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 86)**
- **pub-key-file** -- Copy the public keys to the switch. **(p. 93)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**
- **startup-config** -- Copy data to the switch configuration file. **(p. 93)**
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy **xmodem** -- Use xmodem on the terminal as the data source. **(p. 104)**

- **command-file** -- Copy command script to switch and execute. **(p. 84)**
  - **pc** -- Change CR/LF to PC style. **(p. 92)**
  - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 84)**
  - **pc** -- Change CR/LF to PC style. **(p. 92)**
  - **unix** -- Change CR/LF to unix style. **(p. 101)**
- **flash** -- Copy to primary/secondary flash. **(p. 90)**
  - **cv_flash < primary | secondary >** -- Copy to primary/secondary flash. **(p. 86)**
- **startup-config** -- Copy data to the switch configuration file. **(p. 93)**
  - **pc** -- Change CR/LF to PC style. **(p. 92)**
  - **unix** -- Change CR/LF to unix style. **(p. 101)**

EXAMPLES

Example: copy config tftp

Copy a startup-config file named test-01 from the switch to a UNIX TFTP server at IP address 10.10.28.14:

```
ProCurve(config)# copy config test-01 tftp 10.10.28.14 test-01.txt unix
```

© 2007 Hewlett-Packard Development Company, L.P.

Example: copy flash flash primary

Copy the image in secondary flash to primary flash:

```
ProCurve(config)# copy flash flash primary
```

COMMAND DETAILS

append (p. 83)	filename (p. 86)	startup-config (p. 93)
card (p. 83)	flash (p. 90)	test-only (p. 94)
command-file (p. 84)	image-name (p. 91)	tftp (p. 97)
command-output (p. 84)	manager (p. 91)	tftp-ip (p. 99)
config (p. 84)	master (p. 91)	unix (p. 101)
crash-data (p. 85)	operator (p. 92)	usb (p. 102)
crash-log (p. 85)	pc (p. 92)	xmodem (p. 104)
cv_flash (p. 86)	pub-key-file (p. 93)	
event-log (p. 86)	running-config (p. 93)	

append

- copy tftp pub-key-file *IP-ADDR FILENAME* append

```
Add the key(s) for operator access.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy tftp pub-key-file *IP-ADDR FILENAME* operator append

```
Add the key(s) for access.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy tftp pub-key-file *IP-ADDR FILENAME* manager append

```
Add the key(s) for access.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

card

- copy crash-data *SLOT-ID-RANGE*

```
Enter single slot identifier.
```

Next Available Options:
- **tftp** -- Copy data to a TFTP server.**(p. 97)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
- **usb** -- Copy data to a USB flash drive.**(p. 102)**

- copy crash-log *SLOT-ID-RANGE*

© 2007 Hewlett-Packard Development Company, L.P.

```
Enter single slot identifier.
```

Next Available Options:
- **tftp** -- Copy data to a TFTP server.**(p. 97)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
- **usb** -- Copy data to a USB flash drive.**(p. 102)**

command-file

- copy tftp command-file

```
Copy command script to switch and execute.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy xmodem command-file

```
Copy command script to switch and execute.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

- copy usb command-file

```
Copy command script to switch and execute.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

command-output

- copy command-output *COMMAND-OUTPUT*

```
Specify a CLI command to copy output of.
```

Next Available Options:
- **tftp** -- Copy data to a TFTP server.**(p. 97)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
- **usb** -- Copy data to a USB flash drive.**(p. 102)**

config

- copy tftp config *CONFIG*

```
Copy data to specified configuration file.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

© 2007 Hewlett-Packard Development Company, L.P.

- copy xmodem config *CONFIG*

  ```
  Copy data to specified configuration file.
  ```

  Next Available Options:
  - **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
  - **unix** -- Change CR/LF to unix style.**(p. 101)**
  - **pc** -- Change CR/LF to PC style.**(p. 92)**

- copy config *< config >*

  ```
  Copy named configuration file.
  ```

  Supported Values:
  - **config**

  Next Available Options:
  - **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 84)**
  - **tftp** -- Copy data to a TFTP server.**(p. 97)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**

- copy config *< config >* config *CONFIG*

  ```
  Copy data to specified configuration file.
  ```

crash-data

- copy crash-data

  ```
  Copy the switch crash data file.
  ```

  Next Available Options:
  - **card** -- Enter single slot identifier. (SLOT-ID-RANGE) **(p. 83)**
  - **master** -- Copy from the master card (default).**(p. 91)**
  - **tftp** -- Copy data to a TFTP server.**(p. 97)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
  - **usb** -- Copy data to a USB flash drive.**(p. 102)**

crash-log

- copy crash-log

  ```
  Copy the switch log file.
  ```

  Next Available Options:
  - **card** -- Enter single slot identifier. (SLOT-ID-RANGE) **(p. 83)**
  - **master** -- Copy from the master card (default).**(p. 91)**
  - **tftp** -- Copy data to a TFTP server.**(p. 97)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
  - **usb** -- Copy data to a USB flash drive.**(p. 102)**

© 2007 Hewlett-Packard Development Company, L.P.

cv_flash

- copy tftp flash *IP-ADDR FILENAME < primary | secondary >*

  ```
  Copy to primary/secondary flash.
  ```

  Supported Values:
  - **primary** -- Copy to primary flash.
  - **secondary** -- Copy to secondary flash.

  Next Available Option:
  - **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy xmodem flash *< primary | secondary >*

  ```
  Copy to primary/secondary flash.
  ```

  Supported Values:
  - **primary** -- Copy to primary flash.
  - **secondary** -- Copy to secondary flash.

  Next Available Option:
  - **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy usb flash *IMAGE-NAME < primary | secondary >*

  ```
  Copy to primary/secondary flash.
  ```

  Supported Values:
  - **primary** -- Copy to primary flash.
  - **secondary** -- Copy to secondary flash.

  Next Available Option:
  - **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

event-log

- copy event-log

  ```
  Copy event log file.
  ```

  Next Available Options:
  - **tftp** -- Copy data to a TFTP server.**(p. 97)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
  - **usb** -- Copy data to a USB flash drive.**(p. 102)**

filename

- copy tftp command-file *IP-ADDR FILENAME*

  ```
  Specify filename for the TFTP transfer.
  ```

  Next Available Options:
  - **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

© 2007 Hewlett-Packard Development Company, L.P.

- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

■ copy tftp flash *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:
- **cv_flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 86)**

■ copy tftp pub-key-file *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:
- **append** -- Add the key(s) for operator access.**(p. 83)**
- **operator** -- Replace the key(s) for operator access (default); follow with the 'append' option to add the key(s).**(p. 92)**
- **manager** -- Replace the key(s) for manager access; follow with the 'append' option to add the key(s).**(p. 91)**

■ copy tftp startup-config *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

■ copy tftp config *CONFIG IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

■ copy usb startup-config *FILENAME*

```
Specify filename for the USB transfer.
```

■ copy usb command-file *FILENAME*

```
Specify filename for the USB transfer.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

© 2007 Hewlett-Packard Development Company, L.P.

- copy usb pub-key-file *FILENAME*

```
Specify filename for the USB transfer.
```

- copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

- copy command-output *COMMAND-OUTPUT* usb *FILENAME*

```
Specify filename for the USB transfer.
```

- copy config *< config >* tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

- copy crash-data *SLOT-ID-RANGE* tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy crash-data *SLOT-ID-RANGE* usb *FILENAME*

```
Specify filename for the USB transfer.
```

- copy crash-data master tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy crash-data master usb *FILENAME*

```
Specify filename for the USB transfer.
```

- copy crash-data tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

© 2007 Hewlett-Packard Development Company, L.P.

- copy crash-data usb *FILENAME*

```
Specify filename for the USB transfer.
```

- copy crash-log *SLOT-ID-RANGE* tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy crash-log *SLOT-ID-RANGE* usb *FILENAME*

```
Specify filename for the USB transfer.
```

- copy crash-log master tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy crash-log master usb *FILENAME*

```
Specify filename for the USB transfer.
```

- copy crash-log tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy crash-log usb *FILENAME*

```
Specify filename for the USB transfer.
```

- copy flash tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

- copy flash usb *FILENAME*

```
Specify filename for the USB transfer.
```

- copy running-config tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**

© 2007 Hewlett-Packard Development Company, L.P.

- **pc** -- Change CR/LF to PC style.**(p. 92)**

■ copy running-config usb *FILENAME*

```
Specify filename for the USB transfer.
```

■ copy startup-config tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

■ copy startup-config usb *FILENAME*

```
Specify filename for the USB transfer.
```

■ copy event-log tftp *IP-ADDR FILENAME*

```
Specify filename for the TFTP transfer.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

■ copy event-log usb *FILENAME*

```
Specify filename for the USB transfer.
```

flash

■ copy tftp flash

```
Copy data to the switch system image file.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

■ copy xmodem flash

```
Copy to primary/secondary flash.
```

Next Available Option:
- **cv_flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 86)**

■ copy usb flash

```
Copy data to the switch system image file.
```

Next Available Option:
- **image-name** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 91)**

© 2007 Hewlett-Packard Development Company, L.P.

- copy flash

  ```
  Copy the switch system image file.
  ```

  Next Available Options:
  - **flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 90)**
  - **tftp** -- Copy data to a TFTP server.**(p. 97)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
  - **usb** -- Copy data to a USB flash drive.**(p. 102)**

- copy flash flash *< primary | secondary >*

  ```
  Copy to primary/secondary flash.
  ```

  Supported Values:
  - **primary** -- Copy to primary flash.
  - **secondary** -- Copy to secondary flash.

image-name

- copy usb flash *IMAGE-NAME*

  ```
  Specify filename for the USB transfer.
  ```

  Next Available Option:
  - **cv_flash** < primary | secondary > -- Copy to primary/secondary flash.**(p. 86)**

manager

- copy tftp pub-key-file *IP-ADDR FILENAME* manager

  ```
  Replace the key(s) for manager access; follow with the 'append' option to add the
  key(s).
  ```

  Next Available Options:
  - **append** -- Add the key(s) for access.**(p. 83)**
  - **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

master

- copy crash-data master

  ```
  Copy from the master card (default).
  ```

  Next Available Options:
  - **tftp** -- Copy data to a TFTP server.**(p. 97)**
  - **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
  - **usb** -- Copy data to a USB flash drive.**(p. 102)**

- copy crash-log master

  ```
  Copy from the master card (default).
  ```

  Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **tftp** -- Copy data to a TFTP server.**(p. 97)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
- **usb** -- Copy data to a USB flash drive.**(p. 102)**

operator

- copy tftp pub-key-file *IP-ADDR FILENAME* operator

```
Replace the key(s) for operator access (default); follow with the 'append' option to
 add the key(s).
```

Next Available Options:

- **append** -- Add the key(s) for access.**(p. 83)**
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

pc

- copy tftp command-file *IP-ADDR FILENAME* pc

```
Change CR/LF to PC style.
```

- copy tftp startup-config *IP-ADDR FILENAME* pc

```
Change CR/LF to PC style.
```

- copy tftp config *CONFIG IP-ADDR FILENAME* pc

```
Change CR/LF to PC style.
```

- copy xmodem startup-config pc

```
Change CR/LF to PC style.
```

- copy xmodem command-file pc

```
Change CR/LF to PC style.
```

- copy xmodem config *CONFIG* pc

```
Change CR/LF to PC style.
```

- copy usb command-file *FILENAME* pc

```
Change CR/LF to PC style.
```

- copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR FILENAME* pc

```
Change CR/LF to PC style.
```

- copy command-output *COMMAND-OUTPUT* xmodem pc

```
Change CR/LF to PC style.
```

- copy config *< config >* tftp *IP-ADDR FILENAME* pc

```
Change CR/LF to PC style.
```

- copy config *< config >* xmodem pc

© 2007 Hewlett-Packard Development Company, L.P.

```
Change CR/LF to PC style.
```

- copy running-config tftp *IP-ADDR FILENAME* pc

```
Change CR/LF to PC style.
```

- copy running-config xmodem pc

```
Change CR/LF to PC style.
```

- copy startup-config tftp *IP-ADDR FILENAME* pc

```
Change CR/LF to PC style.
```

- copy startup-config xmodem pc

```
Change CR/LF to PC style.
```

- copy event-log tftp *IP-ADDR FILENAME* pc

```
Change CR/LF to PC style.
```

- copy event-log xmodem pc

```
Change CR/LF to PC style.
```

pub-key-file

- copy tftp pub-key-file

```
Copy the public keys to the switch.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy usb pub-key-file

```
Copy the public keys to the switch.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

running-config

- copy running-config

```
Copy running configuration file.
```

Next Available Options:
- **tftp** -- Copy data to a TFTP server.**(p. 97)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
- **usb** -- Copy data to a USB flash drive.**(p. 102)**

startup-config

- copy tftp startup-config

© 2007 Hewlett-Packard Development Company, L.P.

```
Copy data to the switch configuration file.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy xmodem startup-config

```
Copy data to the switch configuration file.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

- copy usb startup-config

```
Copy data to the switch configuration file.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

- copy startup-config

```
Copy in-flash configuration file.
```

Next Available Options:
- **tftp** -- Copy data to a TFTP server.**(p. 97)**
- **xmodem** -- Use xmodem on the terminal as the data destination.**(p. 104)**
- **usb** -- Copy data to a USB flash drive.**(p. 102)**

test-only

- copy tftp command-file *IP-ADDR FILENAME* test-only

```
Just test data transfer; present in debug images only.
```

- copy tftp flash *IP-ADDR FILENAME* *< primary | secondary >* test-only

```
Just test data transfer; present in debug images only.
```

- copy tftp pub-key-file *IP-ADDR FILENAME* append test-only

```
Just test data transfer; present in debug images only.
```

- copy tftp pub-key-file *IP-ADDR FILENAME* operator append test-only

```
Just test data transfer; present in debug images only.
```

- copy tftp pub-key-file *IP-ADDR FILENAME* operator test-only

```
Just test data transfer; present in debug images only.
```

- copy tftp pub-key-file *IP-ADDR FILENAME* manager append test-only

```
Just test data transfer; present in debug images only.
```

© 2007 Hewlett-Packard Development Company, L.P.

- copy tftp pub-key-file *IP-ADDR FILENAME* manager test-only

  Just test data transfer; present in debug images only.

- copy tftp startup-config *IP-ADDR FILENAME* test-only

  Just test data transfer; present in debug images only.

- copy tftp config *CONFIG IP-ADDR FILENAME* test-only

  Just test data transfer; present in debug images only.

- copy xmodem flash *< primary | secondary >* test-only

  Just test data transfer; present in debug images only.

- copy xmodem startup-config test-only

  Just test data transfer; present in debug images only.

- copy xmodem command-file test-only

  Just test data transfer; present in debug images only.

- copy xmodem config *CONFIG* test-only

  Just test data transfer; present in debug images only.

- copy usb flash *IMAGE-NAME < primary | secondary >* test-only

  Just test data transfer; present in debug images only.

- copy usb command-file *FILENAME* test-only

  Just test data transfer; present in debug images only.

- copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR FILENAME* test-only

  Just test data transfer; present in debug images only.

- copy command-output *COMMAND-OUTPUT* xmodem test-only

  Just test data transfer; present in debug images only.

- copy config *< config >* tftp *IP-ADDR FILENAME* test-only

  Just test data transfer; present in debug images only.

- copy config *< config >* xmodem test-only

  Just test data transfer; present in debug images only.

- copy crash-data *SLOT-ID-RANGE* tftp *IP-ADDR FILENAME* test-only

  Just test data transfer; present in debug images only.

- copy crash-data *SLOT-ID-RANGE* xmodem test-only

  Just test data transfer; present in debug images only.

- copy crash-data master tftp *IP-ADDR FILENAME* test-only

  Just test data transfer; present in debug images only.

© 2007 Hewlett-Packard Development Company, L.P.

- copy crash-data master xmodem test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy crash-data tftp *IP-ADDR FILENAME* test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy crash-data xmodem test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy crash-log *SLOT-ID-RANGE* tftp *IP-ADDR FILENAME* test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy crash-log *SLOT-ID-RANGE* xmodem test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy crash-log master tftp *IP-ADDR FILENAME* test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy crash-log master xmodem test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy crash-log tftp *IP-ADDR FILENAME* test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy crash-log xmodem test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy flash tftp *IP-ADDR FILENAME* test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy flash xmodem test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy running-config tftp *IP-ADDR FILENAME* test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy running-config xmodem test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy startup-config tftp *IP-ADDR FILENAME* test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy startup-config xmodem test-only

  ```
  Just test data transfer; present in debug images only.
  ```

- copy event-log tftp *IP-ADDR FILENAME* test-only

  ```
  Just test data transfer; present in debug images only.
  ```

© 2007 Hewlett-Packard Development Company, L.P.

- copy event-log xmodem test-only

```
Just test data transfer; present in debug images only.
```

tftp

- copy tftp

```
Copy data from a TFTP server.
```

Next Available Options:
- **command-file** -- Copy command script to switch and execute.**(p. 84)**
- **flash** -- Copy data to the switch system image file.**(p. 90)**
- **pub-key-file** -- Copy the public keys to the switch.**(p. 93)**
- **startup-config** -- Copy data to the switch configuration file.**(p. 93)**
- **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 84)**

- copy command-output *COMMAND-OUTPUT* tftp

```
Copy data to a TFTP server.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy config *< config >* tftp

```
Copy data to a TFTP server.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy crash-data *SLOT-ID-RANGE* tftp

```
Copy data to a TFTP server.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy crash-data master tftp

```
Copy data to a TFTP server.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy crash-data tftp

```
Copy data to a TFTP server.
```

Next Available Option:
- **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

© 2007 Hewlett-Packard Development Company, L.P.

- copy crash-log *SLOT-ID-RANGE* tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Option:
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy crash-log master tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Option:
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy crash-log tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Option:
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy flash tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Option:
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy running-config tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Option:
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy startup-config tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Option:
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

- copy event-log tftp

  ```
  Copy data to a TFTP server.
  ```

  Next Available Option:
  - **tftp-ip** -- Specify TFTP server IP address. (IP-ADDR) **(p. 99)**

© 2007 Hewlett-Packard Development Company, L.P.

tftp-ip

- copy tftp command-file *IP-ADDR*

  ```
  Specify TFTP server IP address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy tftp flash *IP-ADDR*

  ```
  Specify TFTP server IP address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy tftp pub-key-file *IP-ADDR*

  ```
  Specify TFTP server IP address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy tftp startup-config *IP-ADDR*

  ```
  Specify TFTP server IP address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy tftp config *CONFIG IP-ADDR*

  ```
  Specify TFTP server IP address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR*

  ```
  Specify TFTP server IP address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy config *< config >* tftp *IP-ADDR*

  ```
  Specify TFTP server IP address.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy crash-data *SLOT-ID-RANGE* tftp *IP-ADDR*

© 2007 Hewlett-Packard Development Company, L.P.

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy crash-data master tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy crash-data tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy crash-log *SLOT-ID-RANGE* tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy crash-log master tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy crash-log tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy flash tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

- copy running-config tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

■ copy startup-config tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

■ copy event-log tftp *IP-ADDR*

```
Specify TFTP server IP address.
```

Next Available Option:
- **filename** -- Specify filename for the TFTP transfer. (ASCII-STR) **(p. 86)**

unix

■ copy tftp command-file *IP-ADDR FILENAME* unix

```
Change CR/LF to unix style.
```

■ copy tftp startup-config *IP-ADDR FILENAME* unix

```
Change CR/LF to unix style.
```

■ copy tftp config *CONFIG IP-ADDR FILENAME* unix

```
Change CR/LF to unix style.
```

■ copy xmodem startup-config unix

```
Change CR/LF to unix style.
```

■ copy xmodem command-file unix

```
Change CR/LF to unix style.
```

■ copy xmodem config *CONFIG* unix

```
Change CR/LF to unix style.
```

■ copy usb command-file *FILENAME* unix

```
Change CR/LF to unix style.
```

■ copy command-output *COMMAND-OUTPUT* tftp *IP-ADDR FILENAME* unix

```
Change CR/LF to unix style.
```

■ copy command-output *COMMAND-OUTPUT* xmodem unix

```
Change CR/LF to unix style.
```

■ copy config *< config >* tftp *IP-ADDR FILENAME* unix

```
Change CR/LF to unix style.
```

© 2007 Hewlett-Packard Development Company, L.P.

- copy config *< config >* xmodem unix

  ```
  Change CR/LF to unix style.
  ```

- copy running-config tftp *IP-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy running-config xmodem unix

  ```
  Change CR/LF to unix style.
  ```

- copy startup-config tftp *IP-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy startup-config xmodem unix

  ```
  Change CR/LF to unix style.
  ```

- copy event-log tftp *IP-ADDR FILENAME* unix

  ```
  Change CR/LF to unix style.
  ```

- copy event-log xmodem unix

  ```
  Change CR/LF to unix style.
  ```

usb

- copy usb

  ```
  Copy data from a USB flash drive.
  ```

  Next Available Options:
  - **startup-config** -- Copy data to the switch configuration file.**(p. 93)**
  - **flash** -- Copy data to the switch system image file.**(p. 90)**
  - **command-file** -- Copy command script to switch and execute.**(p. 84)**
  - **pub-key-file** -- Copy the public keys to the switch.**(p. 93)**

- copy command-output *COMMAND-OUTPUT* usb

  ```
  Copy data to a USB flash drive.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

- copy crash-data *SLOT-ID-RANGE* usb

  ```
  Copy crash data content to a USB flash drive. You can copy individual slot
  information or the master switch information. If you do not specify either,
  the command defaults to the master data.
  ```

  Next Available Option:
  - **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

- copy crash-data master usb

© 2007 Hewlett-Packard Development Company, L.P.

```
Copy crash data content to a USB flash drive. You can copy individual slot
information or the master switch information. If you do not specify either,
the command defaults to the master data.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy crash-data usb

```
Copy crash data content to a USB flash drive. You can copy individual slot
information or the master switch information. If you do not specify either,
the command defaults to the master data.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy crash-log *SLOT-ID-RANGE* usb

```
Copy crash log content to a USB flash drive. You can copy individual slot
information or the master switch information. If you do not specify either,
the command defaults to the master data.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy crash-log master usb

```
Copy crash log content to a USB flash drive. You can copy individual slot
information or the master switch information. If you do not specify either,
the command defaults to the master data.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy crash-log usb

```
Copy crash log content to a USB flash drive. You can copy individual slot
information or the master switch information. If you do not specify either,
the command defaults to the master data.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy flash usb

```
Copy data to a USB flash drive.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy running-config usb

```
Copy running configuration data to a USB flash drive.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy startup-config usb

```
Copy startup configuration data to a USB flash drive.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

■ copy event-log usb

```
Copy event log data to a USB flash drive.
```

Next Available Option:
- **filename** -- Specify filename for the USB transfer. (ASCII-STR) **(p. 86)**

xmodem

■ copy xmodem

```
Use xmodem on the terminal as the data source.
```

Next Available Options:
- **flash** -- Copy to primary/secondary flash.**(p. 90)**
- **startup-config** -- Copy data to the switch configuration file.**(p. 93)**
- **command-file** -- Copy command script to switch and execute.**(p. 84)**
- **config** -- Copy data to specified configuration file. (ASCII-STR) **(p. 84)**

■ copy command-output *COMMAND-OUTPUT* xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

■ copy config *< config >* xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**
- **pc** -- Change CR/LF to PC style.**(p. 92)**

■ copy crash-data *SLOT-ID-RANGE* xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

■ copy crash-data master xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

■ copy crash-data xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

■ copy crash-log *SLOT-ID-RANGE* xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

■ copy crash-log master xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

■ copy crash-log xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

■ copy flash xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Option:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**

■ copy running-config xmodem

```
Use xmodem on the terminal as the data destination.
```

Next Available Options:
- **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
- **unix** -- Change CR/LF to unix style.**(p. 101)**

© 2007 Hewlett-Packard Development Company, L.P.

- **pc** -- Change CR/LF to PC style.**(p. 92)**

- copy startup-config xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

  Next Available Options:
  - **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
  - **unix** -- Change CR/LF to unix style.**(p. 101)**
  - **pc** -- Change CR/LF to PC style.**(p. 92)**

- copy event-log xmodem

  ```
  Use xmodem on the terminal as the data destination.
  ```

  Next Available Options:
  - **test-only** -- Just test data transfer; present in debug images only.**(p. 94)**
  - **unix** -- Change CR/LF to unix style.**(p. 101)**
  - **pc** -- Change CR/LF to PC style.**(p. 92)**

© 2007 Hewlett-Packard Development Company, L.P.

crypto

OVERVIEW

Category:	SSH
Primary context:	config
Related Commands	**show crypto (page 344)**

```
Usage: crypto host-cert generate self-signed [START END CNAME OU ORG
                                              CITY STATE COUNTRY]
       crypto host-cert zeroize
       crypto key generate <ssh [rsa] | cert [rsa] KEYSIZE>
       crypto key zeroize <ssh | cert>

Description: Install or remove authentication files for ssh or https server.

Parameters:

    o host-cert - operation on the https host certificate file. The host
             certificate file cannot be created before the certificate
             rsa key file has been created.
    o key - operation on an ssh or https rsa key file.
    o generate - install new key or self-signed certificate.
             Note: installing a new key may be very slow in the first few
             minutes after booting the device.
    o zeroize - remove an existing key or certificate file.

    o self-signed - install new self-signed certificate.
    o START - certificate will be valid beginning on this date.
    o END - certificate will be valid until this date.
    o CNAME - the name (IP address) of this device.
    o OU - organizational unit or department.
    o ORG - organization name.
    o CITY - city or location.
    o STATE - state or region.
    o COUNTRY - two character ISO country code.  Typing 'x<TAB>' will
             provide a list of all valid country codes beginning with
             the letter x.

    o ssh - Install/remove host key for ssh server.
    o cert - Install/remove rsa key for https certificate.
    o rsa - optional keyword indicating key type (only rsa is available).
    o KEYSIZE - for a certificate key, the size of the key desired.
             Certificate keys may be 512, 768, or 1024 bits.  (Ssh host
             keys are always 896 bits.)
```

COMMAND STRUCTURE

- crypto **host-cert** -- Install/remove self-signed certificate for https. **(p. 114)**
  - **generate** -- Create a self-signed certificate for the https server. **(p. 114)**
    - **self-signed** -- Create a self-signed certificate for the https server. **(p. 115)**
      - **start-date** -- Validity start date for certificate. (MM/DD[/[YY]YY]) **(p. 116)**
        - **end-date** -- Validity end date for certificate. (MM/DD[/[YY]YY]) **(p. 113)**
          - **cname** -- Common name [e.g., IP address of device]. (ASCII-STR) **(p. 109)**
            - **org-unit** -- Organizational unit [Department]. (ASCII-STR) **(p. 115)**

© 2007 Hewlett-Packard Development Company, L.P.

- **organization** -- Organization name. (ASCII-STR) **(p. 115)**
  - *additional options available...*
- **zeroize** -- Delete an existing certificate. **(p. 116)**

■ crypto **key** -- Install/remove RSA key file for ssh or https server. **(p. 114)**

- **generate** -- Generate a new key. **(p. 114)**
  - **cert** -- Install RSA key file for https certificate. **(p. 108)**
    - **key-size < 512 | 768 | 1024 >** -- **(p. 115)**
    - **rsa** -- Optional keyword. **(p. 115)**
      - **key-size < 512 | 768 | 1024 >** -- **(p. 115)**
  - **ssh** -- Install RSA key file for ssh server. **(p. 116)**
    - **rsa** -- Optional keyword. **(p. 115)**
- **zeroize** -- Delete existing key. **(p. 116)**
  - **cert** -- Remove RSA key file for https certificate. **(p. 108)**
  - **ssh** -- Remove RSA key file for ssh server. **(p. 116)**

EXAMPLES

Example: crypto key generate cert

Generate a key and a new host certificate:

```
HPSwitch(config)# crypto key generate cert 512
Installing new RSA key.  If the key/entropy cache is
depleted, this could take up to a minute.
HPSwitch(config)# crypto host-cert generate self-signed
Validity start date [01/01/1970]: 01/01/2002
Validity end date   [01/01/2003]: 01/01/2004
Common name     [10.255.255.255]: 10.255.255.255
Organization      [Company Name]: Hewlett Packard
Organizational unit  [Dept Name]: ProCurve Network
City or location          [City]: Roseville
State name               [State]: Ca
Country code                [US]: US
```

COMMAND DETAILS

cert (p. 108)	**host-cert (p. 114)**	**self-signed (p. 115)**
city (p. 109)	**key (p. 114)**	**ssh (p. 116)**
cname (p. 109)	**key-size (p. 115)**	**start-date (p. 116)**
country (p. 109)	**organization (p. 115)**	**state (p. 116)**
end-date (p. 113)	**org-unit (p. 115)**	**zeroize (p. 116)**
generate (p. 114)	**rsa (p. 115)**	

cert

■ crypto key generate cert

`Install RSA key file for https certificate.`

Next Available Options:

- **rsa** -- Optional keyword.**(p. 115)**
- **key-size** < 512 | 768 | 1024 > -- **(p. 115)**

■ crypto key zeroize cert

`Remove RSA key file for https certificate.`

city

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT ORGANIZATION CITY*

  ```
  City or location.
  ```

  Next Available Option:
  - **state** -- State or region. (ASCII-STR) **(p. 116)**

cname

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME*

  ```
  Common name [e.g., IP address of device].
  ```

  Next Available Option:
  - **org-unit** -- Organizational unit [Department]. (ASCII-STR) **(p. 115)**

country

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT ORGANIZATION CITY STATE < AD | AE | AF | ... >*

  ```
  Country code (2 character ISO code).
  ```

  Supported Values:
  - **AD** -- Andorra
  - **AE** -- United Arab Emirates
  - **AF** -- Afghanistan
  - **AG** -- Antigua and Barbuda
  - **AI** -- Anguilla
  - **AL** -- Albania
  - **AM** -- Armenia
  - **AN** -- Netherlands Antilles
  - **AO** -- Angola
  - **AQ** -- Antarctica
  - **AR** -- Argentina
  - **AS** -- American Samoa
  - **AT** -- Austria
  - **AU** -- Australia
  - **AW** -- Aruba
  - **AZ** -- Azerbaijan
  - **BA** -- Bosnia and Herzegovina
  - **BB** -- Barbados
  - **BD** -- Bangladesh
  - **BE** -- Belgium
  - **BF** -- Burkina Faso
  - **BG** -- Bulgaria
  - **BH** -- Bahrain
  - **BI** -- Burundi
  - **BJ** -- Benin
  - **BM** -- Bermuda
  - **BN** -- Brunei Darussalam

© 2007 Hewlett-Packard Development Company, L.P.

- **BO** -- Bolivia
- **BR** -- Brazil
- **BS** -- Bahamas
- **BT** -- Bhutan
- **BV** -- Bouvet Island
- **BW** -- Botswana
- **BY** -- Belarus
- **BZ** -- Belize
- **CA** -- Canada
- **CC** -- Cocos (Keeling) Islands
- **CF** -- Central African Republic
- **CG** -- Congo
- **CH** -- Switzerland
- **CI** -- Cote D'Ivoire (Ivory Coast)
- **CK** -- Cook Islands
- **CL** -- Chile
- **CM** -- Cameroon
- **CN** -- China
- **CO** -- Colombia
- **CR** -- Costa Rica
- **CU** -- Cuba
- **CV** -- Cape Verde
- **CX** -- Christmas Island
- **CY** -- Cyprus
- **CZ** -- Czech Republic
- **DE** -- Germany
- **DJ** -- Djibouti
- **DK** -- Denmark
- **DM** -- Dominica
- **DO** -- Dominican Republic
- **DZ** -- Algeria
- **EC** -- Ecuador
- **EE** -- Estonia
- **EG** -- Egypt
- **EH** -- Western Sahara
- **ER** -- Eritrea
- **ES** -- Spain
- **ET** -- Ethiopia
- **FI** -- Finland
- **FJ** -- Fiji
- **FK** -- Falkland Islands (Malvinas)
- **FM** -- Micronesia
- **FO** -- Faroe Islands
- **FR** -- France
- **FX** -- France, Metropolitan
- **GA** -- Gabon
- **GB** -- Great Britain (UK)
- **GD** -- Grenada
- **GE** -- Georgia
- **GF** -- French Guiana
- **GH** -- Ghana
- **GI** -- Gibraltar
- **GL** -- Greenland
- **GM** -- Gambia

© 2007 Hewlett-Packard Development Company, L.P.

- **GN** -- Guinea
- **GP** -- Guadeloupe
- **GQ** -- Equatorial Guinea
- **GR** -- Greece
- **GS** -- S. Georgia and S. Sandwich Isls.
- **GT** -- Guatemala
- **GU** -- Guam
- **GW** -- Guinea-Bissau
- **GY** -- Guyanav
- **HK** -- Hong Kong
- **HM** -- Heard and McDonald Islands
- **HN** -- Honduras
- **HR** -- Croatia (Hrvatska)
- **HT** -- Haiti
- **HU** -- Hungary
- **ID** -- Indonesia
- **IE** -- Ireland
- **IL** -- Israel
- **IN** -- India
- **IO** -- British Indian Ocean Territory
- **IQ** -- Iraq
- **IR** -- Iran
- **IS** -- Iceland
- **IT** -- Italy
- **JM** -- Jamaica
- **JO** -- Jordan
- **JP** -- Japan
- **KE** -- Kenya
- **KG** -- Kyrgyzstan
- **KH** -- Cambodia
- **KI** -- Kiribati
- **KM** -- Comoros
- **KN** -- Saint Kitts and Nevis
- **KP** -- Korea (North)
- **KR** -- Korea (South)
- **KW** -- Kuwait
- **KY** -- Cayman Islands
- **KZ** -- Kazakhstan
- **LA** -- Laos
- **LB** -- Lebanon
- **LC** -- Saint Lucia
- **LI** -- Liechtenstein
- **LK** -- Sri Lanka
- **LR** -- Liberia
- **LS** -- Lesotho
- **LT** -- Lithuania
- **LU** -- Luxembourg
- **LV** -- Latvia
- **LY** -- Libya
- **MA** -- Morocco
- **MC** -- Monaco
- **MD** -- Moldova
- **MG** -- Madagascar
- **MH** -- Marshall Islands

© 2007 Hewlett-Packard Development Company, L.P.

- **MK** -- Macedonia
- **ML** -- Mali
- **MM** -- Myanmar
- **MN** -- Mongolia
- **MO** -- Macau
- **MP** -- Northern Mariana Islands
- **MQ** -- Martinique
- **MR** -- Mauritania
- **MS** -- Montserrat
- **MT** -- Malta
- **MU** -- Mauritius
- **MV** -- Maldives
- **MW** -- Malawi
- **MX** -- Mexico
- **MY** -- Malaysia
- **MZ** -- Mozambique
- **NA** -- Namibia
- **NC** -- New Caledonia
- **NE** -- Niger
- **NF** -- Norfolk Island
- **NG** -- Nigeria
- **NI** -- Nicaragua
- **NL** -- Netherlands
- **NO** -- Norway
- **NP** -- Nepal
- **NR** -- Nauru
- **NT** -- Neutral Zone
- **NU** -- Niue
- **NZ** -- New Zealand (Aotearoa)
- **OM** -- Oman
- **PA** -- Panama
- **PE** -- Peru
- **PF** -- French Polynesia
- **PG** -- Papua New Guinea
- **PH** -- Philippines
- **PK** -- Pakistan
- **PL** -- Poland
- **PM** -- St. Pierre and Miquelon
- **PN** -- Pitcairn
- **PR** -- Puerto Rico
- **PT** -- Portugal
- **PW** -- Palau
- **PY** -- Paraguay
- **QA** -- Qatar
- **RE** -- Reunion
- **RO** -- Romania
- **RU** -- Russian Federation
- **RW** -- Rwanda
- **SA** -- Saudi Arabia
- **Sb** -- Solomon Islands
- **SC** -- Seychelles
- **SD** -- Sudan
- **SE** -- Sweden
- **SG** -- Singapore

© 2007 Hewlett-Packard Development Company, L.P.

- **SH** -- St. Helena
- **SI** -- Slovenia
- **SJ** -- Svalbard and Jan Mayen Islands
- **SK** -- Slovak Republic
- **SL** -- Sierra Leone
- **SM** -- San Marino
- **SN** -- Senegal
- **SO** -- Somalia
- **SR** -- Suriname
- **ST** -- Sao Tome and Principe
- **SV** -- El Salvador
- **SY** -- Syria
- **SZ** -- Swaziland
- **TC** -- Turks and Caicos Islands
- **TD** -- Chad
- **TF** -- French Southern Territories
- **TG** -- Togo
- **TH** -- Thailand
- **TJ** -- Tajikistan
- **TK** -- Tokelau
- **TM** -- Turkmenistan
- **TN** -- Tunisia
- **TO** -- Tonga
- **TP** -- East Timor
- **TR** -- Turkey
- **TT** -- Trinidad and Tobago
- **TV** -- Tuvalu
- **TW** -- Taiwan
- **TZ** -- Tanzania
- **UA** -- Ukraine
- **UG** -- Uganda
- **UK** -- United Kingdom
- **UM** -- US Minor Outlying Islands
- **US** -- United States
- **UY** -- Uruguay
- **UZ** -- Uzbekistan
- **VA** -- Vatican City State (Holy See)
- **VC** -- Saint Vincent and the Grenadines
- **VE** -- Venezuela
- **VG** -- Virgin Islands (U.S.)
- **VN** -- Viet Nam
- **VU** -- Vanuatu
- **WF** -- Wallis and Futuna Islands
- **WS** -- Samoa
- **YE** -- Yemen
- **YT** -- Mayotte
- **YU** -- Yugoslavia
- **ZA** -- South Africa
- **ZM** -- Zambia
- **ZR** -- Zaire
- **ZW** -- Zimbabwe

end-date

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE]*

© 2007 Hewlett-Packard Development Company, L.P.

```
Validity end date for certificate.
```

Next Available Option:
- **cname** -- Common name [e.g., IP address of device]. (ASCII-STR) **(p. 109)**

generate

- crypto host-cert generate

```
Create a self-signed certificate for the https server.
```

Next Available Option:
- **self-signed** -- Create a self-signed certificate for the https server.**(p. 115)**

- crypto key generate

```
Generate a new key.
```

Caution

Protect your private key file from access by anyone other than yourself. If someone can access your private key file, they can then penetrate SSH security on the switch by appearing to be you.

SSH does not protect the switch from unauthorized access via the web interface, Telnet, SNMP, or the serial port. While web and Telnet access can be restricted by the use of passwords local to the switch, if you are unsure of the security this provides, you may want to disable web-based and/or Telnet access ("no web-management" and "no telnet"). If you need to increase SNMP security, you should use SNMP version 3 only. To protect against unauthorized access to the serial port, keep physical access to the switch restriced to authorized personnel.

Next Available Options:
- **cert** -- Install RSA key file for https certificate.**(p. 108)**
- **ssh** -- Install RSA key file for ssh server.**(p. 116)**

host-cert

- crypto host-cert

```
Install/remove self-signed certificate for https.
```

Next Available Options:
- **generate** -- Create a self-signed certificate for the https server.**(p. 114)**
- **zeroize** -- Delete an existing certificate.**(p. 116)**

key

- crypto key

```
Install/remove RSA key file for ssh or https server.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **generate** -- Generate a new key.**(p. 114)**
- **zeroize** -- Delete existing key.**(p. 116)**

key-size

- crypto key generate cert rsa *< 512 | 768 | 1024 >*

  Supported Values:
  - **512** -- Install 512-bit RSA key.
  - **768** -- Install 768-bit RSA key.
  - **1024** -- Install 1024-bit RSA key.
- crypto key generate cert *< 512 | 768 | 1024 >*

  Supported Values:
  - **512** -- Install 512-bit RSA key.
  - **768** -- Install 768-bit RSA key.
  - **1024** -- Install 1024-bit RSA key.

organization

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT ORGANIZATION*

  `Organization name.`

  Next Available Option:
  - **city** -- City or location. (ASCII-STR) **(p. 109)**

org-unit

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT*

  `Organizational unit [Department].`

  Next Available Option:
  - **organization** -- Organization name. (ASCII-STR) **(p. 115)**

rsa

- crypto key generate cert rsa

  `Optional keyword.`

  Next Available Option:
  - **key-size** < 512 | 768 | 1024 > -- **(p. 115)**

- crypto key generate ssh rsa

  `Optional keyword.`

self-signed

- crypto host-cert generate self-signed

© 2007 Hewlett-Packard Development Company, L.P.

```
Create a self-signed certificate for the https server.
```

Next Available Option:
- **start-date** -- Validity start date for certificate. (MM/DD[/[YY]YY]) **(p. 116)**

ssh

- crypto key generate ssh

```
Install RSA key file for ssh server.
```

Next Available Option:
- **rsa** -- Optional keyword.**(p. 115)**

- crypto key zeroize ssh

```
Remove RSA key file for ssh server.
```

start-date

- crypto host-cert generate self-signed *[DATE: START-DATE]*

```
Validity start date for certificate.
```

Next Available Option:
- **end-date** -- Validity end date for certificate. (MM/DD[/[YY]YY]) **(p. 113)**

state

- crypto host-cert generate self-signed *[DATE: START-DATE] [DATE: END-DATE] CNAME ORG-UNIT ORGANIZATION CITY STATE*

```
State or region.
```

Next Available Option:
- **country** < AD | AE | AF | ... > -- Country code (2 character ISO code).**(p. 109)**

zeroize

- crypto host-cert zeroize

```
Delete an existing certificate.
```

- crypto key zeroize

```
Delete existing key.
```

Next Available Options:
- **cert** -- Remove RSA key file for https certificate.**(p. 108)**
- **ssh** -- Remove RSA key file for ssh server.**(p. 116)**

© 2007 Hewlett-Packard Development Company, L.P.

debug

OVERVIEW

Category:	
Primary context:	manager
Related Commands	**log (page 239)** **show logging (page 363)** **show debug (page 345)**

```
Usage: [no] debug destination <logging|session>
       [no] debug <all|DEBUG_TYPE>

Description: Enable/disable debug logging.

Parameters:

    o logging - Send the debug messages to a workstation via the syslog
                facility.  System logging must first be enabled with the
                'logging' command.
    o session - Debug messages will be displayed on the current console,
                telnet, or ssh session.
    o all - Display all debug messages.
    o DEBUG_TYPE - Display debug messages of the specified type.  Use
                <TAB> to see a list of available types and sub-types.
```

COMMAND STRUCTURE

- [no] debug **acl** -- Display debug messages on access control lists. **(p. 118)**
- [no] debug **all** -- Display all debug messages. **(p. 118)**
- [no] debug **arp-protect** -- Display Dynamic ARP Protection messages. **(p. 118)**
- [no] debug **destination < logging | session >** -- Select destination for debug messages. **(p. 118)**
- [no] debug **dhcp-snooping** -- Display all DHCP Snooping messages. **(p. 118)**
  - **agent** -- Display DHCP Snooping agent messages. **(p. 118)**
  - **event** -- Display DHCP Snooping event messages. **(p. 119)**
  - **packet** -- Display DHCP Snooping packet messages. **(p. 120)**
- [no] debug **event** -- Display event log messages. **(p. 119)**
- [no] debug **ip** -- Display all IP routing messages. **(p. 119)**
  - **ospf** -- Display all OSPF routing messages. **(p. 119)**
    - **adj** -- Display adjacency changes. **(p. 118)**
    - **event** -- Display OSPF events. **(p. 119)**
    - **flood** -- Display information on flood messages. **(p. 119)**
    - **lsa-generation** -- Display new LSAs added to database. **(p. 119)**
    - **packet** -- Display packets sent/received. **(p. 120)**
    - **retransmission** -- Display retransmission timer messages. **(p. 120)**
    - **spf** -- Display path recalculation messages. **(p. 120)**
  - **rip** -- Display all RIP routing messages. **(p. 120)**
    - **database** -- Display database changes. **(p. 118)**
    - **event** -- Display RIP events. **(p. 119)**
    - **trigger** -- Display trigger messages. **(p. 120)**
- [no] debug **lldp** -- Display LLDP information. **(p. 119)**

© 2007 Hewlett-Packard Development Company, L.P.

COMMAND DETAILS

acl (p. 118)	dhcp-snooping (p. 118)	ospf (p. 119)
adj (p. 118)	event (p. 119)	packet (p. 120)
arp-protect (p. 118)	flood (p. 119)	retransmission (p. 120)
agent (p. 118)	ip (p. 119)	rip (p. 120)
all (p. 118)	lldp (p. 119)	spf (p. 120)
database (p. 118)	lsa-generation (p. 119)	trigger (p. 120)
destination (p. 118)		

acl

- [no] debug acl

  Display debug messages on access control lists.

adj

- [no] debug ip ospf adj

  Display adjacency changes.

agent

- [no] debug dhcp-snooping agent

  Display DHCP Snooping agent messages.

all

- [no] debug all

  Display all debug messages.

arp-protect

- [no] debug arp-protect

  Display Dynamic ARP Protection messages.

database

- [no] debug ip rip database

  Display database changes.

destination

- [no] debug destination *< logging | session >*

  Select destination for debug messages.

  Supported Values:
  - **logging** -- Send debug messages to syslog server.
  - **session** -- Print debug messages to terminal.

dhcp-snooping

- [no] debug dhcp-snooping

© 2007 Hewlett-Packard Development Company, L.P.

```
Display all DHCP Snooping messages.
```

Next Available Options:
- **agent** -- Display DHCP Snooping agent messages.**(p. 118)**
- **event** -- Display DHCP Snooping event messages.**(p. 119)**
- **packet** -- Display DHCP Snooping packet messages.**(p. 120)**

event

- [no] debug event

```
Display event log messages.
```

- [no] debug ip ospf event

```
Display OSPF events.
```

- [no] debug ip rip event

```
Display RIP events.
```

- [no] debug dhcp-snooping event

```
Display DHCP Snooping event messages.
```

flood

- [no] debug ip ospf flood

```
Display information on flood messages.
```

ip

- [no] debug ip

```
Display all IP routing messages.
```

Next Available Options:
- **ospf** -- Display all OSPF routing messages.**(p. 119)**
- **rip** -- Display all RIP routing messages.**(p. 120)**

lldp

- [no] debug lldp

```
Display LLDP information.
```

lsa-generation

- [no] debug ip ospf lsa-generation

```
Display new LSAs added to database.
```

ospf

- [no] debug ip ospf

```
Display all OSPF routing messages.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:
- **adj** -- Display adjacency changes.**(p. 118)**
- **event** -- Display OSPF events.**(p. 119)**
- **flood** -- Display information on flood messages.**(p. 119)**
- **lsa-generation** -- Display new LSAs added to database.**(p. 119)**
- **packet** -- Display packets sent/received.**(p. 120)**
- **retransmission** -- Display retransmission timer messages.**(p. 120)**
- **spf** -- Display path recalculation messages.**(p. 120)**

packet

- [no] debug ip ospf packet

  ```
  Display packets sent/received.
  ```

- [no] debug dhcp-snooping packet

  ```
  Display DHCP Snooping packet messages.
  ```

retransmission

- [no] debug ip ospf retransmission

  ```
  Display retransmission timer messages.
  ```

rip

- [no] debug ip rip

  ```
  Display all RIP routing messages.
  ```

  Next Available Options:
  - **database** -- Display database changes.**(p. 118)**
  - **event** -- Display RIP events.**(p. 119)**
  - **trigger** -- Display trigger messages.**(p. 120)**

spf

- [no] debug ip ospf spf

  ```
  Display path recalculation messages.
  ```

trigger

- [no] debug ip rip trigger

  ```
  Display trigger messages.
  ```

© 2007 Hewlett-Packard Development Company, L.P.

dhcp-relay

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] dhcp-relay
       [no] dhcp-relay [hop-count-increment]
       dhcp-relay [option 82 append[validate]|replace[validate]
                        |drop[validate]|keep [mac|ip]]
       [no] dhcp-relay [option 82 [validate]]

Description: Enable/disable DHCP relay agent on the device.

 hop-count-increment  --- optional argument to 'dhcp-relay' command used to
                  enable/disable increment of hop-count. By default it is
                  enabled.
 option 82    --- optional argument to 'dhcp-relay' command used to specify
                  the operational status (enable/disable) of option 82.
 append|replace|keep|drop ---    argument to 'option 82' command used to
                  specify the policy to apply to client DHCP packets. There
                  is no default option 82 policy defined for the switch.
 validate     --- optional argument to 'option 82' append, replace, and drop
                  sub-arguments used to specify that a validation of the
                  server response packets such that at least one option 82
                  field matches the remote ID of the current switch (multiple
                  option 82 fields may exist, if relay agent is configured
                  using the append policy).
                  If validation fails, the response is considered invalid and
                  thrown away.
 mac          --- Sets the remote ID to be the MAC address of the switch.
                  This is the default value.
 ip           --- Sets the remote ID to be the IP address of the VLAN on
                  which the client request was received.
```

COMMAND STRUCTURE

- [no] dhcp-relay **hop-count-increment** -- Optional argument to dhcp-agent used to enable/disable increment of DHCP hop-count field. **(p. 124)**
- [no] dhcp-relay **option** -- Optional argument to dhcp-agent used to specify operational status for DHCP options. **(p. 126)**
  - **82** -- Optional argument to dhcp-agent used to specify the operational status for option 82. **(p. 123)**
    - **append** -- Specifies that the option 82 field should be appended to client DHCP packet. **(p. 123)**
      - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 124)**
      - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 125)**
      - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 125)**
      - **validate** -- Specifies the validation for server response. **(p. 126)**
    - **drop** -- Specifies that the DHCP packet will be dropped unconditionally, if option 82 field(s) already exists in the client DHCP packet. **(p. 123)**

© 2007 Hewlett-Packard Development Company, L.P.

- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 124)**
- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 125)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 125)**
- **validate** -- Specifies the validation for server response. **(p. 126)**

- **keep** -- Specifies that no option 82 field will be added or replaced, if option 82 field(s) already exists in the client DHCP packet. **(p. 124)**
  - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 124)**
  - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 125)**
  - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 125)**
- **replace** -- Specifies that any existing option 82 fields will be replaced with switch option 82 field for client DHCP packet. **(p. 126)**
  - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 124)**
  - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 125)**
  - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 125)**
  - **validate** -- Specifies the validation for server response. **(p. 126)**
- **validate** -- Specifies the validation for server response. **(p. 126)**
  - **append** -- Specifies that the option 82 field should be appended to client DHCP packet. **(p. 123)**
    - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 124)**
    - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 125)**
    - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 125)**
  - **drop** -- Specifies that the DHCP packet will be dropped unconditionally, if option 82 field(s) already exists in the client DHCP packet. **(p. 123)**
    - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 124)**
    - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 125)**
    - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 125)**
  - **replace** -- Specifies that any existing option 82 fields will be replaced with switch option 82 field for client DHCP packet. **(p. 126)**
    - **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received. **(p. 124)**
    - **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value. **(p. 125)**
    - **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN. **(p. 125)**

COMMAND DETAILS

82 (p. 123)	**ip (p. 124)**	**option (p. 126)**
append (p. 123)	**keep (p. 124)**	**replace (p. 126)**
drop (p. 123)	**mac (p. 125)**	**validate (p. 126)**
hop-count-increment (p. 124)	**mgmt-vlan (p. 125)**	

© 2007 Hewlett-Packard Development Company, L.P.

82

- [no] dhcp-relay option 82

```
Optional argument to dhcp-agent used to specify the operational status
for option 82.
```

Next Available Options:

- **append** -- Specifies that the option 82 field should be appended to client DHCP packet.**(p. 123)**
- **replace** -- Specifies that any existing option 82 fields will be replaced with switch option 82 field for client DHCP packet.**(p. 126)**
- **keep** -- Specifies that no option 82 field will be added or replaced, if option 82 field(s) already exists in the client DHCP packet.**(p. 124)**
- **drop** -- Specifies that the DHCP packet will be dropped unconditionally, if option 82 field(s) already exists in the client DHCP packet.**(p. 123)**
- **validate** -- Specifies the validation for server response.**(p. 126)**

append

- dhcp-relay option 82 append

```
Specifies that the option 82 field should be appended to client DHCP
packet.
```

Next Available Options:

- **validate** -- Specifies the validation for server response.**(p. 126)**
- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 125)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 124)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 125)**

- dhcp-relay option 82 validate append

```
Specifies that the option 82 field should be appended to client DHCP
packet.
```

Next Available Options:

- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 125)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 124)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 125)**

drop

- dhcp-relay option 82 drop

```
Specifies that the DHCP packet will be dropped unconditionally, if
option 82 field(s) already exists in the client DHCP packet.
```

Next Available Options:

- **validate** -- Specifies the validation for server response.**(p. 126)**
- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 125)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 124)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 125)**

© 2007 Hewlett-Packard Development Company, L.P.

- dhcp-relay option 82 validate drop

```
Specifies that the DHCP packet will be dropped unconditionally, if
option 82 field(s) already exists in the client DHCP packet.
```

Next Available Options:

- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 125)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 124)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 125)**

hop-count-increment

- [no] dhcp-relay hop-count-increment

```
Optional argument to dhcp-agent used to enable/disable increment of
DHCP hop-count field.
```

ip

- dhcp-relay option 82 append ip

```
Sets the remote id to be the IP address of the VLAN on which the client
request was received.
```

- dhcp-relay option 82 replace ip

```
Sets the remote id to be the IP address of the VLAN on which the client
request was received.
```

- dhcp-relay option 82 keep ip

```
Sets the remote id to be the IP address of the VLAN on which the client
request was received.
```

- dhcp-relay option 82 drop ip

```
Sets the remote id to be the IP address of the VLAN on which the client
request was received.
```

- dhcp-relay option 82 validate append ip

```
Sets the remote id to be the IP address of the VLAN on which the client
request was received.
```

- dhcp-relay option 82 validate replace ip

```
Sets the remote id to be the IP address of the VLAN on which the client
request was received.
```

- dhcp-relay option 82 validate drop ip

```
Sets the remote id to be the IP address of the VLAN on which the client
request was received.
```

keep

- dhcp-relay option 82 keep

© 2007 Hewlett-Packard Development Company, L.P.

```
Specifies that no option 82 field will be added or replaced, if option 82
field(s) already exists in the client DHCP packet.
```

Next Available Options:

- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 125)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 124)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 125)**

mac

- dhcp-relay option 82 append mac

```
Sets the remote id to be the MAC address of the switch. This is the
default value.
```

- dhcp-relay option 82 replace mac

```
Sets the remote id to be the MAC address of the switch. This is the
default value.
```

- dhcp-relay option 82 keep mac

```
Sets the remote id to be the MAC address of the switch. This is the
default value.
```

- dhcp-relay option 82 drop mac

```
Sets the remote id to be the MAC address of the switch. This is the
default value.
```

- dhcp-relay option 82 validate append mac

```
Sets the remote id to be the MAC address of the switch. This is the
default value.
```

- dhcp-relay option 82 validate replace mac

```
Sets the remote id to be the MAC address of the switch. This is the
default value.
```

- dhcp-relay option 82 validate drop mac

```
Sets the remote id to be the MAC address of the switch. This is the
default value.
```

mgmt-vlan

- dhcp-relay option 82 append mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 replace mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 keep mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

© 2007 Hewlett-Packard Development Company, L.P.

- dhcp-relay option 82 drop mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 validate append mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 validate replace mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

- dhcp-relay option 82 validate drop mgmt-vlan

```
Sets the remote id to be the IP address of the Management VLAN.
```

option

- [no] dhcp-relay option

```
Optional argument to dhcp-agent used to specify operational status for
DHCP options.
```

Next Available Option:

- **82** -- Optional argument to dhcp-agent used to specify the operational status for option 82.**(p. 123)**

replace

- dhcp-relay option 82 replace

```
Specifies that any existing option 82 fields will be replaced with
 switch option 82 field for client DHCP packet.
```

Next Available Options:

- **validate** -- Specifies the validation for server response.**(p. 126)**
- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 125)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 124)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 125)**

- dhcp-relay option 82 validate replace

```
Specifies that any existing option 82 fields will be replaced with
 switch option 82 field for client DHCP packet.
```

Next Available Options:

- **mac** -- Sets the remote id to be the MAC address of the switch. This is the default value.**(p. 125)**
- **ip** -- Sets the remote id to be the IP address of the VLAN on which the client request was received.**(p. 124)**
- **mgmt-vlan** -- Sets the remote id to be the IP address of the Management VLAN.**(p. 125)**

validate

- dhcp-relay option 82 append validate

© 2007 Hewlett-Packard Development Company, L.P.

```
Specifies the validation for server response.
```

- dhcp-relay option 82 replace validate

```
Specifies the validation for server response.
```

- dhcp-relay option 82 drop validate

```
Specifies the validation for server response.
```

- [no] dhcp-relay option 82 validate

```
Specifies the validation for server response.
```

Next Available Options:

- **append** -- Specifies that the option 82 field should be appended to client DHCP packet.**(p. 123)**
- **replace** -- Specifies that any existing option 82 fields will be replaced with switch option 82 field for client DHCP packet.**(p. 126)**
- **drop** -- Specifies that the DHCP packet will be dropped unconditionally, if option 82 field(s) already exists in the client DHCP packet.**(p. 123)**

© 2007 Hewlett-Packard Development Company, L.P.

dhcp-snooping

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] dhcp-snooping

Description: Enable/Disable the global administrative status of
             DHCP snooping. No snooping will be performed on
             any VLAN if the global administrative status is disabled.
             The default state is disabled.
```

COMMAND STRUCTURE

- [no] dhcp-snooping **authorized-server** -- Configure valid DHCP Servers **(p. 129)**
  - **IP-ADDR** -- DHCP Server address. (IP-ADDR) **(p. 130)**
- [no] dhcp-snooping **database** -- Configure lease database transfer options **(p. 129)**
  - **delay < 15 to 86400 >** -- Seconds to delay writing to the lease database file. **(p. 129)**
  - **file** -- URL Format: "tftp://<ip-address>/<filename>". (ASCII-STR) **(p. 130)**
  - **timeout < 0 to 86400 >** -- Seconds to wait for the transfer before failing. **(p. 131)**
- [no] dhcp-snooping **option** -- Configure DHCP snooping operational behavior **(p. 130)**
  - **82** -- **(p. 128)**
    - **remote-id < mac | subnet-ip | mgmt-ip >** -- Set relay information option remote-id value to use. (NUMBER) **(p. 131)**
    - **untrusted-policy < drop | keep | replace >** -- Policy for DHCP packets received on untrusted ports thatcontain option 82. (NUMBER) **(p. 131)**
- [no] dhcp-snooping **trust** -- Configure trusted interfaces **(p. 131)**
  - **port-list** -- ([ethernet] PORT-LIST) **(p. 131)**
- [no] dhcp-snooping **verify** -- Enable/Disable DHCP packet validation **(p. 131)**
  - **mac** -- Verify DHCP header client hardware address. **(p. 130)**
- [no] dhcp-snooping **vlan** -- Enable/Disable snooping on a VLAN (VLAN-ID-RANGE) **(p. 132)**
  - **vlan-list** -- (VLAN-ID-RANGE) **(p. 132)**

COMMAND DETAILS

82 (p. 128)	**IP-ADDR (p. 130)**	**untrusted-policy (p. 131)**
authorized-server (p. 129)	**option (p. 130)**	**verify (p. 131)**
database (p. 129)	**port-list (p. 131)**	**vlan (p. 132)**
delay (p. 129)	**remote-id (p. 131)**	**vlan-list (p. 132)**
file (p. 130)	**timeout (p. 131)**	
mac (p. 130)	**trust (p. 131)**	

82

- [no] dhcp-snooping option 82

  Next Available Options:
  - **untrusted-policy** < drop | keep | replace > -- Policy for DHCP packets received on untrusted ports that contain option 82. (NUMBER) **(p. 131)**
  - **remote-id** < mac | subnet-ip | mgmt-ip > -- Set relay information option remote-id value to use. (NUMBER) **(p. 131)**

© 2007 Hewlett-Packard Development Company, L.P.

authorized-server

- [no] dhcp-snooping authorized-server

```
Usage: [no] dhcp-snooping authorized-server <IP-ADDR>

Description: Configure valid DHCP Servers.
             For DHCP Snooping to allow a server to client packet
             to be forwarded, it must be received on a trusted port
             from a valid server. If no authorized servers are configured
             all server addresses are valid. A maximum of 20 authorized
             servers are supported.

Parameters:

    o IP-ADDR - The Address of a trusted DHCP Server.
```

Next Available Option:

- **IP-ADDR** -- DHCP Server address. (IP-ADDR) **(p. 130)**

database

- [no] dhcp-snooping database

```
Usage: [no] dhcp-snooping database [file ASCII-STR] [delay  <15-86400>]
                                   [timeout <0-86400>]

Description: Configure lease database transfer options.

             No additional parameters required when 'no' is specified.

Parameters:

    o [file ASCI-STR] - File name in the form of a Universal Resource Locator.
                        The URL must be "tftp://IP-ADDR/ASCII-STR".
                        The max filename length is 63 characters.

    o [delay  <15-86400>]  - Number of seconds to delay writing the database.
                             The default delay is 300 seconds

    o [timeout <0-86400>]  - Number of seconds to wait for the database file
                             transfer to finish before declaring an error.
                             A value of 0 means retry indefinitely.
                             The default timeout is 300 seconds
```

Next Available Options:

- **file** -- URL Format: "tftp://<ip-address>/<filename>". (ASCII-STR) **(p. 130)**
- **delay** < 15 to 86400 > -- Seconds to delay writing to the lease database file.**(p. 129)**
- **timeout** < 0 to 86400 > -- Seconds to wait for the transfer before failing.**(p. 131)**

delay

- dhcp-snooping database delay *< 15 to 86400 >*

```
Seconds to delay writing to the lease database file.
```

© 2007 Hewlett-Packard Development Company, L.P.

Range: < 15 to 86400 >

file

- dhcp-snooping database file *FILE*

```
URL Format: "tftp://<ip-address>/<filename>".
```

IP-ADDR

- [no] dhcp-snooping authorized-server *IP-ADDR*

```
DHCP Server address.
```

mac

- [no] dhcp-snooping verify mac

```
Verify DHCP header client hardware address.
```

option

- [no] dhcp-snooping option

```
Usage: [no] dhcp-snooping option 82 [remote-id <mac|subnet-ip|mgmt-ip>]
                                    [untrusted-policy <drop|keep|replace>]

Description: Configure DHCP snooping operational behavior.

Parameters:

    o 82 - Add relay information option to DHCP client packets
           that are being forwarded out trusted ports. When 'no'
           is specified, relay information is not inserted.
           The default is to insert relay information.

    o [remote-id <mac|mgmt-ip|subnet-ip>]
         - Set the value used for the remote-id field of the
           relay information option. If 'mac' is specified,
           the switch mac address is used. If 'mgmt-ip' is
           specified, the management vlan ip address is used.
           If 'subnet-ip' is specified, the ip address of the
           VLAN the packet was received on is used. Note that
           when the specified value is 'subnet-ip' or 'mgmt-ip'
           and that value is not set, then the switch mac address
           will be used. The default remote-id is the switch mac.

    o [untrusted-policy <drop|keep|replace>]
         - Configures snooping behavior when forwarding a DHCP
           packet from an untrusted port that has a DHCP relay
           information option present. If 'drop' is specified, the
           packet is dropped. If 'keep' is specified, the packet
           is forwarded without replacing the option. If 'replace'
           is specified the existing option is replaced with one
           generated by this switch. The default is to drop.
```

Next Available Option:

- **82** -- **(p. 128)**

port-list

- [no] dhcp-snooping trust *[ETHERNET] PORT-LIST*

remote-id

- dhcp-snooping option 82 remote-id *< mac | subnet-ip | mgmt-ip >*

```
Set relay information option remote-id value to use.
```

Supported Values:
- **mac** -- switch MAC address.
- **subnet-ip** -- subnet VLAN IP address.
- **mgmt-ip** -- management VLAN IP address.

timeout

- dhcp-snooping database timeout *< 0 to 86400 >*

```
Seconds to wait for the transfer before failing.
```

Range: < 0 to 86400 >

trust

- [no] dhcp-snooping trust

```
Usage: [no] dhcp-snooping trust PORT-LIST

Description: Configure trusted interfaces. Only server packets received
             on trusted interfaces will be forwarded. When 'no' is
             specified the interfaces are marked as untrusted.
             The default port state is untrusted.

Parameters:

    o PORT-LIST - Port list on which to configure trust status.
```

Next Available Option:
- **port-list** -- ([ethernet] PORT-LIST) **(p. 131)**

untrusted-policy

- dhcp-snooping option 82 untrusted-policy *< drop | keep | replace >*

```
Policy for DHCP packets received on untrusted ports thatcontain option 82.
```

Supported Values:
- **drop** -- drop the packet.
- **keep** -- forward the packet unchanged.
- **replace** -- generate new option.

verify

- [no] dhcp-snooping verify

```
Usage: [no] dhcp-snooping verify <mac>

Description: Enable/Disable DHCP packet validation.

Parameters:
```

© 2007 Hewlett-Packard Development Company, L.P.

```
    o <mac> - Verify DHCP header client hardware address field
              and the source mac address match for packets received
              on untrusted ports. If 'no' is specified this check is
              omitted. The default is to verify the macs.
```

Next Available Option:

- **mac** -- Verify DHCP header client hardware address.**(p. 130)**

vlan

- dhcp-snooping vlan

```
Usage: [no] dhcp-snooping vlan [VLAN-ID-RANGE ...]
Description: Enable/Disable snooping on a VLAN.
             Note that DHCP snooping must also be globally
             enabled with the 'dhcp-snooping' command for
             snooping to performed on any VLAN. The default state
             is disabled.
Parameters:
    o VLAN-ID-RANGE - VLAN list on which to enable/disable snooping.
```

Next Available Option:

- **vlan-list** -- (VLAN-ID-RANGE) **(p. 132)**

vlan-list

- [no] dhcp-snooping vlan *VLAN-ID-RANGE*

© 2007 Hewlett-Packard Development Company, L.P.

dir

OVERVIEW

Category:	
Primary context:	operator
Related Commands	

```
Usage: dir [<pathname>]

Description: Display a list of the files and subdirectories in a
             directory on a USB device.
```

COMMAND STRUCTURE

- dir **pathname** -- Display a list of the files and subdirectories in a directory on a USB device (ASCII-STR) **(p. 133)**

COMMAND DETAILS

pathname (p. 133)

pathname

- dir *PATHNAME*

```
Usage: dir [<pathname>]

Description: Display a list of the files and subdirectories in a
             directory on a USB device.
```

© 2007 Hewlett-Packard Development Company, L.P.

enable

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	**exit (page 138)** **end (page 135)**

```
Usage: enable

Description: Enter the Manager Exec context.
```

EXAMPLES

Example: enable

Enter the Manager user name and password to access the Manager Exec context of the CLI:

```
ProCurve> enable
Username: admin1
Password: ########
ProCurve#
```

© 2007 Hewlett-Packard Development Company, L.P.

end

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**exit (page 138)** **enable (page 134)**

```
Usage: end

Description: Return to the Manager Exec context.
```

NOTES

To Exit from a Context

To exit from any context of the CLI to the previous context, use the "exit" command.

© 2007 Hewlett-Packard Development Company, L.P.

erase

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show config (page 341)** **show port-access (page 371)**

```
Usage: erase <startup-config |
              flash <primary|secondary> |
              config FILENAME>

Description: Erase files from flash memory. You can erase configuration files or
             flash images.

Parameters:
    o startup-config - erases the configuration file loaded
             at the most recent boot.  This will cause an immediate
             reboot with a factory-default configuration.
    o flash <primary|secondary> - erases the specified software image from flash
             memory.
    o config FILENAME - erases the specified configuration file.  If
             the config file erased is the one loaded at the most
             recent boot, this will cause an immediate reboot using
             the factory-default configuration.
```

COMMAND STRUCTURE

- erase **config < config1 >** -- Erase the named configuration file **(p. 136)**
- erase **flash < primary | secondary >** -- Erase the primary or secondary flash image **(p. 137)**
- erase **startup-config** -- Erase configuration file. **(p. 137)**

EXAMPLES

Example: erase startup-config

Erase the configuration file used at startup and reset the device to its factory-default configuration:

```
ProCurve(config)# erase startup-config
Configuration will be deleted and device rebooted, continue [y/n]?
```

COMMAND DETAILS

config (p. 136)	**flash (p. 137)**	**startup-config (p. 137)**

config

- erase config *< config1 >*

```
Usage: erase config FILENAME

Description: Erase the named configuration file.
```

Supported Values:

© 2007 Hewlett-Packard Development Company, L.P.

- **config1**

flash

- erase flash *< primary | secondary >*

```
Usage: erase flash <primary|secondary>

Description: Erase the primary or secondary flash image.
```

Supported Values:
- **primary** -- Primary flash image.
- **secondary** -- Secondary flash image.

startup-config

- erase startup-config

```
Erase configuration file.
```

© 2007 Hewlett-Packard Development Company, L.P.

exit

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	**end (page 135)** **enable (page 134)**

```
Usage: exit

Description: Return to the previous context or terminate current
             console/telnet session if you are in the Operator context
             level.
```

NOTES

Exit to Manager Exec Context

To exit directly from any configuration context to the Manager Exec context, you can use the "end" command instead.

EXAMPLES

Example: exit

Exit from the interface configuration context to the global configuration context:

```
ProCurve(eth-A4)# exit
ProCurve(config)#
```

© 2007 Hewlett-Packard Development Company, L.P.

fastboot

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] fastboot

Description: Enable/disable fastboot on switch. The fastboot command allows
             a boot sequence that skips the internal power-on self-tests,
             resulting in a faster boot time.
```

© 2007 Hewlett-Packard Development Company, L.P.

fault-finder

OVERVIEW

Category:	
Primary context:	config
Related Commands	**interface (page 158)** **show interfaces (page 358)**

```
Usage: [no] fault-finder <all|bad-driver|bad-transceiver|bad-cable|
                          too-long-cable|over-bandwidth|broadcast-storm|
                          loss-of-link>
                         [sensitivity <low|medium|high>]

Description: Enable or disable the switch to detect physical layer or network
             faults.
             Enable setting of sensitivity. Default is 'sensitivity medium'.
```

COMMAND STRUCTURE

- [no] fault-finder **fault-finder < all | bad-driver | bad-transceiver | ... >** -- Enable/disable fault finder and set sensitivity **(p. 140)**
- fault-finder **sensitivity < low | medium | high >** -- Define fault finder sensitivity to events. **(p. 140)**

COMMAND DETAILS

fault-finder (p. 140)	**sensitivity (p. 140)**

fault-finder

- [no] fault-finder *< all | bad-driver | bad-transceiver | ... >*

```
Usage: [no] fault-finder <all|bad-driver|bad-transceiver|bad-cable|
                          too-long-cable|over-bandwidth|broadcast-storm|
                          loss-of-link>
                         [sensitivity <low|medium|high>]

Description: Enable/disable fault finder and set sensitivity.
             Default is 'sensitivity medium'.
```

Supported Values:

- **all** -- All fault types.
- **bad-driver** -- Too many undersized/giant packets.
- **bad-transceiver** -- Excessive jabbering.
- **bad-cable** -- Excessive CRC/alignment errors.
- **too-long-cable** -- Excessive late collisions.
- **over-bandwidth** -- High collision or drop rate.
- **broadcast-storm** -- Excessive broadcasts.
- **loss-of-link** -- Link lost detected.
- **duplex-mismatch-HDx** -- Duplex Mismatch. Reconfig port to Full Duplex.
- **duplex-mismatch-FDx** -- Duplex Mismatch. Reconfig port to Auto.

sensitivity

- fault-finder sensitivity *< low | medium | high >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Define fault finder sensitivity to events.
```

Supported Values:

- **low** -- Low sensitivity.
- **medium** -- Medium sensitivity.
- **high** -- High sensitivity.

© 2007 Hewlett-Packard Development Company, L.P.

filter

OVERVIEW

Category:	Troubleshooting
Primary context:	config
Related Commands	**connection-rate-filter (page 73)** **ip (page 180)** **show filter (page 349)** **show connection-rate-filter (page 344)**

```
Usage: [no] filter ...

Description: Set or edit traffic/security filters.
             The command allows you to set conditional filters and
             corresponding actions to apply to the incoming traffic.
             These actions will meet the specified conditions.
             Use 'filter ?' to get a list of all available
             filter types.
```

COMMAND STRUCTURE

- [no] filter **connection-rate** -- Selects behavior for port(s) when a host is filtered **(p. 143)**
  - **connection-rate-portlist** -- ([ethernet] PORT-LIST) **(p. 143)**
    - **filter-action < block | notify-only | throttle >** -- **(p. 144)**
- [no] filter **multicast** -- Specify multicast filter to manage (MAC-ADDR) **(p. 145)**
  - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**
  - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
- [no] filter **protocol < ip | ipx | arp | ... >** -- Specify protocol filter to manage **(p. 146)**
  - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**
  - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
- [no] filter **source-port** -- Specify source-port filter to manage **(p. 146)**
  - **named-filter** -- Set the filter name. **(p. 145)**
    - **ascii** -- Set the filter name. (ASCII-STR) **(p. 143)**
      - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**
      - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
  - **port-list** -- Set the list of source port filters. ([ethernet] PORT-LIST) **(p. 145)**
    - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**
      - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
    - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
      - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**
    - **named-filter** -- Set the filter name. (ASCII-STR) **(p. 145)**

© 2007 Hewlett-Packard Development Company, L.P.

EXAMPLES

Example: filter source-port drop

Create a source-port filter that drops all traffic received on port 5 with a destination of port trunk 1 (trk1) and any port in the range of port 10 to port 15:

```
ProCurve(config)# filter source-port 5 drop trk1,A10-A15
```

Example: filter source-port drop

Create a filter on port trunk 1 to drop traffic received inbound for trunk 2 (trk2) and ports 10-15:

```
ProCurve(config)# filter source-port trk1 drop trk2,A10-A15
```

COMMAND DETAILS

ascii (p. 143)	**filter-action (p. 144)**	**port-list (p. 145)**
connection-rate (p. 143)	**forward (p. 144)**	**protocol (p. 146)**
connection-rate-portlist (p. 143)	**multicast (p. 145)**	**source-port (p. 146)**
drop (p. 144)	**named-filter (p. 145)**	

ascii

- [no] filter source-port named-filter *ASCII*

```
Set the filter name.
```

Next Available Options:

- **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
- **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**

connection-rate

- [no] filter connection-rate

```
Usage: [no] filter connection-rate port-list  < notify-only | throttle | block>

Description: Selects behavior for port(s) when a host is filtered.
             Block will disable the host until an administrator explicitly
             re-enables access.  Throttle will deny network access for a
             specific penalty period before automatically re-enabling
             access.  Notify will simply log a message/send a SNMP
             trap when the filter is tripped.
```

Next Available Option:

- **connection-rate-portlist** -- ([ethernet] PORT-LIST) **(p. 143)**

connection-rate-portlist

- [no] filter connection-rate *[ETHERNET] PORT-LIST*

Next Available Option:

- **filter-action** < block | notify-only | throttle > -- **(p. 144)**

© 2007 Hewlett-Packard Development Company, L.P.

drop

- filter source-port named-filter *ASCII* drop *[ETHERNET] PORT-LIST*

  ```
  Set a list of ports to which forwarding of filtered packets is not permitted.
  ```

- filter source-port *[ETHERNET] PORT-LIST* forward *[ETHERNET] PORT-LIST* drop *[ETHERNET] PORT-LIST*

  ```
  Set a list of ports to which forwarding of filtered packets is not permitted.
  ```

- filter source-port *[ETHERNET] PORT-LIST* drop *[ETHERNET] PORT-LIST*

  ```
  Set a list of ports to which forwarding of filtered packets is not permitted.
  ```

  Next Available Option:
  - **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**

- filter multicast *MAC-ADDR* drop *[ETHERNET] PORT-LIST*

  ```
  Set a list of ports to which forwarding of filtered packets is not permitted.
  ```

- filter protocol *< ip | ipx | arp | ... >* drop *[ETHERNET] PORT-LIST*

  ```
  Set a list of ports to which forwarding of filtered packets is not permitted.
  ```

filter-action

- filter connection-rate *[ETHERNET] PORT-LIST < block | notify-only | throttle >*

  Supported Values:
  - **block** -- Disable the host until an administrator explicitly re-enables access.
  - **notify-only** -- Log a message/send a SNMP trap when the filter is tripped.
  - **throttle** -- Deny network access for a period before automatically re-enabling access.

forward

- filter source-port named-filter *ASCII* forward *[ETHERNET] PORT-LIST*

  ```
  Set a list of ports to which forwarding of filtered packets is permitted.
  ```

- filter source-port *[ETHERNET] PORT-LIST* forward *[ETHERNET] PORT-LIST*

  ```
  Set a list of ports to which forwarding of filtered packets is permitted.
  ```

  Next Available Option:
  - **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**

- filter source-port *[ETHERNET] PORT-LIST* drop *[ETHERNET] PORT-LIST* forward *[ETHERNET] PORT-LIST*

  ```
  Set a list of ports to which forwarding of filtered packets is permitted.
  ```

- filter multicast *MAC-ADDR* forward *[ETHERNET] PORT-LIST*

© 2007 Hewlett-Packard Development Company, L.P.

```
Set a list of ports to which forwarding of filtered packets is permitted.
```

- filter protocol *< ip | ipx | arp | ... >* forward *[ETHERNET] PORT-LIST*

```
Set a list of ports to which forwarding of filtered packets is permitted.
```

multicast

- [no] filter multicast *MAC-ADDR*

```
Usage: [no] filter multicast MAC-ADDR [...]

Description: Specify multicast filter to manage.
             If preceded by 'no' the command deletes the filter specified.
             Otherwise, the filter is added to the system, if
             it is not already there. Also, an action to apply to the
             packets satisfying to the filter condition can be set.
             The packets satisfying to the filter condition are all
             packets destined to the MAC-ADDR specified. Use
             'filter source-port [ethernet] PORT-NUM ?' to get a list
             of all possible actions that could be applied to the packets.
```

Next Available Options:

- **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
- **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**

named-filter

- [no] filter source-port named-filter

```
Set the filter name.
```

Next Available Option:

- **ascii** -- Set the filter name. (ASCII-STR) **(p. 143)**

- filter source-port *[ETHERNET] PORT-LIST* named-filter *NAMED-FILTER*

```
Set the filter name.
```

port-list

- [no] filter source-port *[ETHERNET] PORT-LIST*

```
Set the list of source port filters.
```

Next Available Options:

- **named-filter** -- Set the filter name. (ASCII-STR) **(p. 145)**
- **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
- **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**

© 2007 Hewlett-Packard Development Company, L.P.

protocol

- [no] filter protocol *< ip | ipx | arp | ... >*

```
Usage: [no] filter protocol <ip|ipx|arp|appletalk|sna|netbeui> [...]

Description: Specify protocol filter to manage.
             If preceded by 'no' the command deletes the filter specified.
             Otherwise, the filter is added to the system, if
             it is not already there. Also, an action to apply to the
             packets satisfying to the filter condition can be set.
             The packets satisfying to the filter condition are all
             packets of the protocol specified. Use 'filter source-port
             [ethernet] PORT-NUM ?' to get a list of all possible actions
             that could be applied to the packets.
```

Supported Values:

- **ip**
- **ipx**
- **arp**
- **appletalk**
- **sna**
- **netbeui**

Next Available Options:

- **forward** -- Set a list of ports to which forwarding of filtered packets is permitted. ([ethernet] PORT-LIST) **(p. 144)**
- **drop** -- Set a list of ports to which forwarding of filtered packets is not permitted. ([ethernet] PORT-LIST) **(p. 144)**

source-port

- [no] filter source-port

```
Usage: [no] filter source-port [...]

Description: Specify source-port filter to manage.
             Create a named filter,associate source port-list to a
             named-filter and apply actions.The named filter can only be 20
             characters long. If source port filter is not named,then
             portname is considered as a filter name, and  apply actions to
             received packet on port. If preceded by 'no' the command
             deletes the filter specified.To delete a named-filter use
             no filter source-port named-filter <filter-name> explicitly.
```

Next Available Options:

- **named-filter** -- Set the filter name.**(p. 145)**
- **port-list** -- Set the list of source port filters. ([ethernet] PORT-LIST) **(p. 145)**

© 2007 Hewlett-Packard Development Company, L.P.

front-panel-security

OVERVIEW

Category:	Switch Security
Primary context:	config
Related Commands	

```
Usage: [no] front_panel_security
            <password-clear [reset-on-clear] |
             factory-reset |
             password-recovery>

Description: Enable/disable the ability to clear the password(s) and/or
             configuration via the front panel buttons.  If 'password-clear' is
             disabled, the password(s) cannot be reset using the clear button on
             the front panel of the device.  If 'factory-reset' is disabled, the
             configuration/password(s) can not be reset using the clear and
             reset button combination at boot time.  With 'password-recovery'
             enabled (and the front panel buttons disabled), a lost password can
             be recovered by contacting HP customer support.  With 'password-
             recovery' disabled, there is no way to access a device after losing
             a password with the front panel buttons disabled.
```

COMMAND STRUCTURE

- [no] front-panel-security **factory-reset** -- Enable/Disable factory-reset ability **(p. 147)**
- [no] front-panel-security **password-clear** -- Enable/Disable password clear **(p. 148)**
  - **reset-on-clear** -- Reset switch on password clear **(p. 148)**
- [no] front-panel-security **password-recovery** -- Enable/Disable password recovery **(p. 148)**

EXAMPLES

Example: no front-panel-security password-recovery

Disable the password-recovery option:

```
HPswitch(config)# no front-panel-security password-recovery
                            **** CAUTION ****
Disabling the clear button without password recovery prevents switch passwords
from being reset.  If the switch password is lost, restoring the default factory
configuration will be required to regain access!

Continue with disabling password recovery [y/n]? y

HPswitch(config)# _
```

COMMAND DETAILS

factory-reset (p. 147)	**password-recovery (p. 148)**
password-clear (p. 148)	**reset-on-clear (p. 148)**

factory-reset

- [no] front-panel-security factory-reset

```
Enable/Disable factory-reset ability
```

© 2007 Hewlett-Packard Development Company, L.P.

password-clear

- [no] front-panel-security password-clear

```
Enable/Disable password clear
```

Next Available Option:

- **reset-on-clear** -- Reset switch on password clear **(p. 148)**

password-recovery

- [no] front-panel-security password-recovery

```
Enable/Disable password recovery
```

reset-on-clear

- [no] front-panel-security password-clear reset-on-clear

```
Reset switch on password clear
```

© 2007 Hewlett-Packard Development Company, L.P.

getMIB

OVERVIEW

Category:	manager
Primary context:	manager
Related Commands	**walkMIB (page 495)**

```
Usage: getmib OBJECT-STR [OBJECT-STR ...]

Description: Retrieve and display the value of the MIB objects specified.
```

COMMAND STRUCTURE

- getMIB **object** -- Name and instance of the MIB variable to retrieve. (ASCII-STR) **(p. 149)**

COMMAND DETAILS

object (p. 149)

object

- getMIB *OBJECT*

  ```
  Name and instance of the MIB variable to retrieve.
  ```

© 2007 Hewlett-Packard Development Company, L.P.

gvrp

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**interface (page 158)** **show gvrp (page 351)**

```
Usage: [no] gvrp

Description: Enable/disable GARP VLAN Registration Protocol (GVRP).
```

EXAMPLES

Example: gvrp

Enable GVRP on the switch:

```
ProCurve(config)# gvrp
```

© 2007 Hewlett-Packard Development Company, L.P.

hostname

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**snmp-server (page 395)**

```
Usage: hostname ASCII-STR

Description: Specify the device name for administrative purposes. The
             ASCII-STR defines the device name. It can be up to 30
             characters. Use quotes if your device name contains
             spaces.
```

EXAMPLES

Example: hostname

Name the switch "Blue" with "Next-4474" as the system contact, and "North-Data-Room" as the location:

```
HPswitch(config)# hostname Blue
Blue(config)# snmp-server contct Ext-4474 location North-Data-Room
Blue(config)# show system-information
 Status and Counters - General System Information

  System Name         : Blue
  System Contact      : Ext-4474
  System Location     : North-Data-Room

  MAC Age Time (sec)  : 300

  Time Zone           : 0
  Daylight Time Rule  : None


  Firmware revision   : E.08.30          Base MAC Addr       : 0001e7-a0ec00
  ROM Version         : E.05.04          Serial Number       : SG00394041


  Up Time             : 14 mins          Memory    - Total   : 25,038,312
  CPU Util (%)        : 1                           Free    : 20,087,448

  IP Mgmt   - Pkts Rx : 0                Packet    - Total   : 832
              Pkts Tx : 0                Buffers     Free    : 783
                                                     Lowest  : 768
-- MORE --, next page: Space, next line: Enter, quit: Control-C
```

© 2007 Hewlett-Packard Development Company, L.P.

igmp

OVERVIEW

Category:	IGMP
Primary context:	config
Related Commands	**show igmp (page 353)**

```
Usage: igmp ...

Description: Configure various global IGMP parameters for the switch. The
             'igmp' command must be followed by a feature-specific keyword.
             Use 'igmp ?' to get a list of all possible options.
```

COMMAND STRUCTURE

- igmp **delayed-flush < 0 to 255 >** -- Configures the number of seconds an empty IGMP Multicast Group filter will persist in hardware after the last group member leaves **(p. 152)**

COMMAND DETAILS

delayed-flush (p. 152)

delayed-flush

- igmp delayed-flush *< 0 to 255 >*

```
Usage: igmp delayed-flush <0..255>

Description: Configures the number of seconds an empty IGMP Multicast
             Group filter will persist in hardware after the last group
             member leaves. This Delayed Group Flush will drop any further
             'stale' traffic for that group until the timer expires. A
             value of 0 (the default behavior) indicates that the feature
             is disabled.
```

Range: < 0 to 255 >

© 2007 Hewlett-Packard Development Company, L.P.

igmp-proxy-domain

OVERVIEW

Category:	IGMP
Primary context:	config
Related Commands	**show igmp-proxy (page 354)** **vlan (page 457)**

```
Usage: [no] igmp-proxy-domain DOMAIN-NAME [BORDER-ROUTER-IP-ADDR
       <MCAST-LOW-IP-ADDR MCAST-HIGH-IP-ADDR|all>]

Description: Configure an IGMP proxy domain.
             If the 'no' keyword is used:
                 The DOMAIN-NAME must be specified, All other parameters
                 are optional (they will be verified if they are
                 specified). The specified domain will be deleted if
                 no VLAN associations exist for it.
             If the 'no' keyword is not used:
                 If the DOMAIN-NAME matches the domain name of an
                 existing domain, the respective domain will be updated
                 to reflect the other parameters. Pre-existing proxy
                 entries that are inconsistent after the update will be
                 removed.
                 If the DOMAIN-NAME does not match the domain name of an
                 existing domain, a new domain will be created.
             MCAST-LOW-IP-ADDR and MCAST-HIGH-IP-ADDR
             refer to the low and high inclusive multicast bounds
             respectively. If the keyword 'all' is specified,
             224.0.1.0-239.255.255.255 is used for the inclusive
             multicast bounds.
```

COMMAND STRUCTURE

- [no] igmp-proxy-domain **domain-name** -- Specify the igmp proxy domain name to be added/deleted/updated. (ASCII-STR) **(p. 154)**
  - **border-ip** -- Specify the igmp proxy border ip address. (IP-ADDR) **(p. 154)**
    - **all** -- Specify ALL if the multicast range 224.0.1.0-239.255.255.255 is desired. **(p. 153)**
    - **mcast-low-ip** -- Specify the igmp proxy multicast low bound (inclusive) ip address. (IP-ADDR) **(p. 154)**
      - **mcast-high-ip** -- Specify the igmp proxy multicast high bound (inclusive) ip address. (IP-ADDR) **(p. 154)**

COMMAND DETAILS

all (p. 153)	**domain-name (p. 154)**	**mcast-low-ip (p. 154)**
border-ip (p. 154)	**mcast-high-ip (p. 154)**	

all

- [no] igmp-proxy-domain *DOMAIN-NAME IP-ADDR* all

```
Specify ALL if the multicast range 224.0.1.0-239.255.255.255 is desired.
```

© 2007 Hewlett-Packard Development Company, L.P.

border-ip

- [no] igmp-proxy-domain *DOMAIN-NAME IP-ADDR*

```
Specify the igmp proxy border ip address.
```

Next Available Options:

- **mcast-low-ip** -- Specify the igmp proxy multicast low bound (inclusive) ip address. (IP-ADDR) **(p. 154)**
- **all** -- Specify ALL if the multicast range 224.0.1.0-239.255.255.255 is desired. **(p. 153)**

domain-name

- [no] igmp-proxy-domain *DOMAIN-NAME*

```
Specify the igmp proxy domain name to be added/deleted/updated.
```

Next Available Option:

- **border-ip** -- Specify the igmp proxy border ip address. (IP-ADDR) **(p. 154)**

mcast-high-ip

- [no] igmp-proxy-domain *DOMAIN-NAME IP-ADDR IP-ADDR IP-ADDR*

```
Specify the igmp proxy multicast high bound (inclusive) ip address.
```

mcast-low-ip

- [no] igmp-proxy-domain *DOMAIN-NAME IP-ADDR IP-ADDR*

```
Specify the igmp proxy multicast low bound (inclusive) ip address.
```

Next Available Option:

- **mcast-high-ip** -- Specify the igmp proxy multicast high bound (inclusive) ip address. (IP-ADDR) **(p. 154)**

© 2007 Hewlett-Packard Development Company, L.P.

instrumentation

OVERVIEW

Category:	config
Primary context:	config
Related Commands	

```
Usage: [no] instrumentation monitor [ [<all|arp-requests|ip-address-count|
                                       learn-discards|login-failures|mac-moves|
                                       mac-address-count|pkts-to-closed-ports|
                                       port-auth-failures|system-resource-usage|
                                       system-delay> [<low|med|high|limitValue>]] ]
       [no] instrumentation monitor [trap]
       [no] instrumentation monitor [log]

Description: Enables/Disables instrumentation monitoring.
             The "instrumentatation monitor" command enables or disables instrumentation

              monitoring and sets the threshold value. By default, instrumentation
              monitoring for all parameters is disabled. The command
              'instrumentation monitor all' sets the threshold of each parameter
              to its medium values. The single command 'instrumentation monitor'
              enables or disables instrumentation monitoring for all parameters
              and also enables or disables the instrumentation monitoring log.
              The second option, "trap", enables or disables
              SNMP trap generation. By default, SNMP trap generation is disabled.
              Traps are generated if SNMP trap is enabled and the counter value
              of the monitoring parameter exceeds the threshold value.
              The third option, "log", enables or disables the
              instrumentation monitoring log. By default, the instrumentation
              monitoring log is disabled.

Parameters:

    o all - Enables/Disables instrumentation monitoring for all parameters.
    o arp-requests - Number of ARP requests received.
    o ip-address-count - Number of destination IP addresses learned in the
      IP forwarding table.
    o learn-discards - Number of MAC address learn events per minute
      discarded to help free CPU resources when busy.
    o login-failures - The count of failed CLI login attempts or
      SNMP management authentication failures.
    o mac-moves - The average number of MAC address moves from one port
      to another per minute.
    o mac-address-count - Number of MAC addresses learned in the
      forwarding table.
    o pkts-to-closed-ports - This could indicate a port scan, in which
      an attacker is attempting to expose a vulnerability in the switch.
    o port-auth-failures - The count of times a client has been unsuccessful
      logging into the network.
    o system-resource-usage - Percentage of system resources in use.
    o system-delay - The response time of the CPU to new network events.

    o low - Preconfigured low threshold value.
    o med - Preconfigured medium threshold value.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
    o high - Preconfigured high threshold value.
    o limitValue - User configured threshold value.
```

COMMAND STRUCTURE

- [no] instrumentation **collection** -- **(p. 156)**
- [no] instrumentation **monitor** -- Enables/Disables instrumentation monitoring **(p. 156)**
  - **log** -- Enables/Disables instrumenation monitoring log. **(p. 156)**
  - **monitor < all | arp-requests | ip-address-count | ... >** -- Enables/Disables instrumentation monitoring **(p. 156)**
    - **limitValue < 1 to 2147483647 >** -- Set the threshold Value. (NUMBER) **(p. 156)**
    - **threshold-value < low | med | high >** -- Set the threshold Value. **(p. 157)**
  - **trap** -- Enables/Disables SNMP trap generation. **(p. 157)**

COMMAND DETAILS

collection (p. 156)	**log (p. 156)**	**threshold-value (p. 157)**
limitValue (p. 156)	**monitor (p. 156)**	**trap (p. 157)**

collection

- [no] instrumentation collection

limitValue

- instrumentation monitor *< all | arp-requests | ip-address-count | ... > < 1 to 2147483647 >*

```
Set the threshold Value.
```

Range: < 1 to 2147483647 >

log

- [no] instrumentation monitor log

```
Enables/Disables instrumenation monitoring log.
```

monitor

- [no] instrumentation monitor

```
Usage: [no] instrumentation monitor [ [<all|arp-requests|ip-address-count|
                                       learn-discards|login-failures|mac-moves|
                                       mac-address-count|pkts-to-closed-ports|
                                       port-auth-failures|system-resource-usage|
                                       system-delay> [<low|med|high|limitValue>]] ]
       [no] instrumentation monitor [trap]
       [no] instrumentation monitor [log]

Description: Enables/Disables instrumentation monitoring.
             The first version of the command enables/disables instrumentation
             monitoring and sets threshold value. By default instrumentation
             monitoring for all parameter is disabled. The command
             'instrumentation monitor all' sets the threshold of each parameter
             to their medium values. The single command 'instrumentation monitor'
             enables/disables instrumentation monitoring for all parameters
             and also enables/disables instrumentation monitoring log.
             The second version of the command enables/disables
             SNMP trap generation. By default SNMP trap generation is disabled.
             Traps are generated if SNMP trap is enabled and counter value
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                of the monitoring parameter exceeds the threshold value.
                The third version of the command enables/disables
                instrumentation monitoring log. By default instrumentation
                monitoring log is disabled.

        Parameters:

            o all - Enables/Disables instrumentation monitoring for all parameters.
            o arp-requests - Number of ARP requests received.
            o ip-address-count - Number of destination IP addresses learned in the
              IP forwarding table.
            o learn-discards - Number of MAC address learn events per minute
              discarded to help free CPU resources when busy.
            o login-failures - The count of failed CLI login attempts or
              SNMP management authentication failures.
            o mac-moves - The average number of MAC address moves from one port
              to another per minute.
            o mac-address-count - Number of MAC addresses learned in the
              forwarding table.
            o pkts-to-closed-ports - This could indicate a port scan, in which
              an attacker is attempting to expose a vulnerability in the switch.
            o port-auth-failures - The count of times a client has been unsuccessful
              logging into the network.
            o system-resource-usage - Percentage of system resources in use.
            o system-delay - The response time of the CPU to new network events.

            o low - Preconfigured low threshold value.
            o med - Preconfigured medium threshold value.
            o high - Preconfigured high threshold value.
            o limitValue - User configured threshold value.
```

Next Available Options:

- **trap** -- Enables/Disables SNMP trap generation. **(p. 157)**
- **log** -- Enables/Disables instrumentation monitoring log. **(p. 156)**

threshold-value

- instrumentation monitor *< all | arp-requests | ip-address-count | ... > < low | med | high >*

```
Set the threshold Value.
```

Supported Values:

- **low** -- Low threshold.
- **med** -- Medium threshold.
- **high** -- High threshold.

trap

- [no] instrumentation monitor trap

```
Enables/Disables SNMP trap generation.
```

© 2007 Hewlett-Packard Development Company, L.P.

interface

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] interface < [ethernet] PORT-LIST [...] | loopback <num> >

Description: Configure settings on the switch's interfaces.
             You can enter the commands form the global configuration context or
             the Interface configuration context.
             To enter an interface command from the global configuration context,
             use the following options in the command to specify the port(s):
             interface [etherner] PORT-LIST.
             To enter interface commands at the interface configuration context,
             type the following as a command to change to the Interface configuration
             context, then type the options as commands:
                interface [ethernet] PORT-LIST.
             Using the "loopback" option will change the context to loopback
             mode.
             Use 'interface ?' to get a list of all valid commands.
```

COMMAND STRUCTURE

- [no] interface **loopback < 0 to 7 >** -- Enter the loopback Configuration Level **(p. 168)**
  - **ip** -- Configure various IP parameters for the Loopback **(p. 166)**
    - **address** -- Set IP parameters for communication within an IP network **(p. 161)**
      - **ip-addr** -- Interface IP address. (IP-ADDR) **(p. 167)**
    - **ospf** -- configure Open Shortest Path First (OSPF) protocol parameters on the interface **(p. 171)**
      - **all** -- Process the request for all IP addresses. **(p. 161)**
        - **area** -- Specify an OSPF area. **(p. 162)**
          - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 162)**
          - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 163)**
        - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 164)**
      - **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 167)**
        - **area** -- Specify an OSPF area. **(p. 162)**
          - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 162)**
          - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 163)**
        - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 164)**
- [no] interface **port-list** -- Enter the Interface Configuration Level, or execute one command for that level ([ethernet] PORT-LIST) **(p. 172)**
  - **arp-protect** -- Configure the port as trusted or untrusted **(p. 162)**
    - **trust** -- **(p. 178)**
  - **bandwidth-min** -- Enable/disable and configure guaranteed minimum bandwidth settings for outgoing traffic on the port(s) **(p. 163)**
    - **output** -- Enable/disable and configure guaranteed minimum bandwidth for outgoing traffic. **(p. 171)**

© 2007 Hewlett-Packard Development Company, L.P.

- queue1 < 0 to 100 > -- Specify min. bandwidth percentage for queue one outgoing traffic. (p. 174)
  - queue2 < 0 to 100 > -- Specify min. bandwidth percentage for queue two outgoing traffic. (p. 174)
    - queue3 < 0 to 100 > -- Specify min. bandwidth percentage for queue three outgoing traffic. (p. 174)
      - queue4 < 0 to 100 > -- Specify min. bandwidth percentage for queue four outgoing traffic. (p. 174)
        - queue5 < 0 to 100 > -- Specify min. bandwidth percentage for queue five outgoing traffic. (p. 175)
          - *additional options available...*

- broadcast-limit < 0 to 99 > -- Set a broadcast traffic percentage limit (p. 164)
- dhcp-snooping -- Configure the port as trusted or untrusted (p. 164)
  - trust -- Configure trusted interfaces (p. 178)
- disable -- Disable port(s) (p. 165)
- enable -- Enable port(s) (p. 165)
- flow-control -- Enable/disable flow control on the port(s) (p. 165)
- gvrp -- Set the GVRP timers on the port (hundreths of a second) (p. 165)
  - join-timer < 20 to 75 > -- Set join timer value (centiseconds; default 20). (p. 167)
  - leaveall-timer < 500 to 3000 > -- Set leaveall timer value (centiseconds; default 1000). (p. 167)
  - leave-timer < 40 to 300 > -- Set leave timer value (centiseconds; default 300). (p. 168)
- ip -- Apply the specified access control list to inbound packets on this INTERFACE list (p. 166)
  - access-group -- Apply the specified access control list to inbound packets on this INTERFACE list (ASCII-STR) (p. 160)
    - direction < in > -- (p. 164)
- lacp -- Define whether LACP is enabled on the port, and whether it is in active or passive mode when enabled (p. 167)
  - mode < Active | Passive > -- Define whether LACP is enabled on the port, and whether it is in active or passive mode when enabled (p. 169)
- link-keepalive -- Configure UDLD on port(s) (p. 168)
  - vlan -- Set vlan-id for tagged UDLD control packets. (VLAN-ID) (p. 179)
- mdix-mode < mdi | mdix | autoMDIX > -- Set port MDI/MDIX mode (default: auto). (p. 168)
- monitor -- Define either the port is to be monitored or not (p. 169)
  - all < In | Out | Both > -- Monitor all traffic. (p. 161)
    - mirror -- Mirror destination. (p. 168)
      - mirror_session_name -- Mirror destination name. (p. 169)
      - monitor_mirror_session_id < 1 to 4 > -- Mirror destination number. (p. 170)
  - ip -- Apply an IPv4 access list. (p. 166)
    - access-group -- Define the mirror port for diagnostic purposes (ASCII-STR) (p. 160)
      - monitor_mirror_ACL_dir < In > -- Define the mirror port for diagnostic purposes (p. 170)
        - mirror -- Mirror destination. (p. 168)
          - mirror_session_name -- Mirror destination name. (p. 169)
          - monitor_mirror_session_id < 1 to 4 > -- Mirror destination number. (p. 170)
- name -- Set/unset a name for the port(s) (p. 170)
  - port-name -- Specify a port name up to 64 characters length. (ASCII-STR) (p. 173)
- power -- Enable/Disable per-port power distribution (p. 173)
  - priority < Critical | High | Low > -- Enable/Disable per-port power distribution (p. 173)
- qos -- Set port-based priority (p. 173)
  - dscp < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. (p. 165)
  - priority < 0 | 1 | 2 | ... > -- Specify priority to use. (p. 173)

© 2007 Hewlett-Packard Development Company, L.P.

- **rate-limit** -- Enable/disable and configure rate-limiting for all traffic (or for incoming ICMP traffic) on the port(s) **(p. 176)**
  - **all** -- Set limits for all traffic. **(p. 161)**
    - **in** -- Set limits for all inbound traffic. **(p. 166)**
      - **bps < 0 to -94967296 >** -- Specify limit as bits-per-second of allowed inbound or outbound traffic. (NUMBER) **(p. 163)**
      - **percent < 0 to 100 >** -- Specify limit as percent of inbound or outbound traffic. **(p. 171)**
    - **out** -- Set limits for all outbound traffic. **(p. 171)**
      - **bps < 0 to -94967296 >** -- Specify limit as bits-per-second of allowed inbound or outbound traffic. (NUMBER) **(p. 163)**
      - **percent < 0 to 100 >** -- Specify limit as percent of inbound or outbound traffic. **(p. 171)**
  - **icmp** -- Set limits for ICMP traffic only. **(p. 166)**
    - **per-port < 0 to 100 >** -- Specify limit as percent of incoming ICMP traffic. **(p. 172)**
- **speed-duplex < 10-half | 100-half | 10-full | ... >** -- Define mode of operation for the port(s) **(p. 176)**
- **type < Trunk | | | ... >** -- **(p. 178)**
- **unknown-vlans < Learn | Block | Disable >** -- Configure GVRP on the port(s) **(p. 178)**

COMMAND DETAILS

access-group (p. 160)	**ip-addr (p. 167)**	**port-list (p. 172)**
address (p. 161)	**join-timer (p. 167)**	**port-name (p. 173)**
all (p. 161)	**lacp (p. 167)**	**power (p. 173)**
area (p. 162)	**leaveall-timer (p. 167)**	**priority (p. 173)**
area-id (p. 162)	**leave-timer (p. 168)**	**qos (p. 173)**
arp-protect (p. 162)	**link-keepalive (p. 168)**	**queue1 (p. 174)**
backbone (p. 163)	**loopback (p. 168)**	**queue2 (p. 174)**
bandwidth-min (p. 163)	**mdix-mode (p. 168)**	**queue3 (p. 174)**
bps (p. 163)	**mirror (p. 168)**	**queue4 (p. 174)**
broadcast-limit (p. 164)	**mirror_session_name (p. 169)**	**queue5 (p. 175)**
cost (p. 164)	**mode (p. 169)**	**queue6 (p. 175)**
dhcp-snooping (p. 164)	**monitor (p. 169)**	**queue7 (p. 175)**
direction (p. 164)	**monitor_mirror_ACL_dir (p. 170)**	**queue8 (p. 175)**
disable (p. 165)	**monitor_mirror_session_id (p. 170)**	**rate-limit (p. 176)**
dscp (p. 165)	**name (p. 170)**	**speed-duplex (p. 176)**
enable (p. 165)	**ospf (p. 171)**	**trust (p. 178)**
flow-control (p. 165)	**out (p. 171)**	**type (p. 178)**
gvrp (p. 165)	**output (p. 171)**	**unknown-vlans (p. 178)**
icmp (p. 166)	**percent (p. 171)**	**vlan (p. 179)**
in (p. 166)	**per-port (p. 172)**	
ip (p. 166)		

access-group

- [no] interface *[ETHERNET] PORT-LIST* ip access-group *ACCESS-GROUP*

```
Usage: [no] ip access-group <ACL-ID> in

Description: Apply the specified access control list to inbound
             packets on this INTERFACE list.  The access
             control list ACL-ID must be defined before it can be applied.
```

Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **direction** < in > -- **(p. 164)**

■ interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Next Available Option:
- **monitor_mirror_ACL_dir** < In > -- Define the mirror port for diagnostic purposes**(p. 170)**

address

■ [no] interface loopback *< 0 to 7 >* ip address

```
Usage: [no] ip address [IP-ADDR]

Description: Set IP parameters for communication within an IP network.
             Each loopback Interface represents an IP interface having
              its own unique configuration.  The loopback interface
             for which the configuration is applied can be specified
             implicitly by preceding the phrase 'ip address' with the
             'interface loopback <num>' keyword and argument.  It
             can also be called explicitly when called directly from a
             Loopback context.  In the latter case the command
             affects the interface identified by the context.

Parameters:

    o IP-ADDR- Assign an IP address to the loopback interface.
      Multiple addresses may be configured on a single loopback interface.
```

Next Available Option:
- **ip-addr** -- Interface IP address. (IP-ADDR) **(p. 167)**

all

■ [no] interface *[ETHERNET] PORT-LIST* monitor all *< In | Out | Both >*

```
Monitor all traffic.
```

Supported Values:
- **In** -- Monitor all inbound traffic
- **Out** -- Monitor all outbound traffic

© 2007 Hewlett-Packard Development Company, L.P.

- **Both** -- Monitor all inbound and outbound traffic

Next Available Option:
- **mirror** -- Mirror destination.**(p. 168)**

■ [no] interface *[ETHERNET] PORT-LIST* rate-limit all

```
Set limits for all traffic.
```

Next Available Options:
- **in** -- Set limits for all inbound traffic.**(p. 166)**
- **out** -- Set limits for all outbound traffic.**(p. 171)**

■ [no] interface loopback *< 0 to 7 >* ip ospf all

```
Process the request for all IP addresses.
```

Next Available Options:
- **area** -- Specify an OSPF area.**(p. 162)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 164)**

area

■ interface loopback *< 0 to 7 >* ip ospf *IP-ADDR* area

```
Specify an OSPF area.
```

Next Available Options:
- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 162)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 163)**

■ interface loopback *< 0 to 7 >* ip ospf all area

```
Specify an OSPF area.
```

Next Available Options:
- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 162)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 163)**

area-id

■ interface loopback *< 0 to 7 >* ip ospf *IP-ADDR* area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

■ interface loopback *< 0 to 7 >* ip ospf all area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

arp-protect

■ interface arp-protect trust

© 2007 Hewlett-Packard Development Company, L.P.

```
Configure the port as trusted or untrusted. ARP traffic received on the
untrusted interfaces of ARP Protection-enabled VLANs are validated against
the set of known IP-to-MAC bindings maintained by DHCP snooping. By
specifying "no" the port is configured as untrusted.
Default: untrusted
```

backbone

- interface loopback *< 0 to 7 >* ip ospf *IP-ADDR* area backbone

```
The backbone area (the same as 0.0.0.0).
```

- interface loopback *< 0 to 7 >* ip ospf all area backbone

```
The backbone area (the same as 0.0.0.0).
```

bandwidth-min

- interface *[ETHERNET] PORT-LIST* bandwidth-min

```
Usage: bandwidth-min output <0-100> <0-100> <0-100> <0-100>
                            <0-100> <0-100> <0-100> <0-100>
       no bandwidth-min output

Description: Enable/disable and configure guaranteed minimum bandwidth
             settings for outgoing traffic on the port(s). By default,
             guaranteed minimum bandwidth is configured with a recommended
             profile for outgoing traffic that prevents higher-priority
             queues from starving lower-priority traffic.
             When the feature is enabled, the value for each of the
             queues indicates the minimum percentage of port throughput that
             will be guaranteed for that queue. If a given queue does not
             require its guaranteed minimum in a given service window, any
             extra bandwidth is allocated to the other queues, beginning
             with the highest-priority queue.
             The actual number of queues could be 2, 4 or 8, depending on
             system default and command 'qos queue-config N-queues'.
             The sum of all configured queue values must not exceed 100%.
             Per-queue values must be specified starting with queue one
             being the lowest priority and queue eight being the highest
             priority.
             If no guaranteed minimum bandwidth is configured (i.e., the
             settings for all queues are 0), the traffic is serviced
             strictly by priority. In practice, this may cause complete
             starvation of some or all lower-priority queues during any
             periods where the output port traffic is over-subscribed.
             This is an Interface context command. It can be called directly
             from the interface context, or following the
             'interface [ethernet] PORT-LIST' command.
```

Next Available Option:

- **output** -- Enable/disable and configure guaranteed minimum bandwidth for outgoing traffic.**(p. 171)**

bps

- interface *[ETHERNET] PORT-LIST* rate-limit all in bps *< 0 to -94967296 >*

```
Specify limit as bits-per-second of allowed inbound or outbound traffic.
```

© 2007 Hewlett-Packard Development Company, L.P.

Range: < 0 to -94967296 >

- interface *[ETHERNET] PORT-LIST* rate-limit all out bps *< 0 to -94967296 >*

```
Specify limit as bits-per-second of allowed inbound or outbound traffic.
```

Range: < 0 to -94967296 >

broadcast-limit

- interface *[ETHERNET] PORT-LIST* broadcast-limit *< 0 to 99 >*

```
Usage: broadcast-limit <0-99>

Description: Set a broadcast traffic percentage limit.
             This command sets the theoretical maximum of network
             bandwidth in percentage that can be used for broadcast
             traffic. Any broadcast traffic exceeding that limit will be
             dropped. '0' means the feature is disabled.
             For 1000 Mbps and higher speed ports, the percentage of broadcast
             traffic configured is that percentage applied to the theoretical
             maximum broadcast throughput for a 100 Mbps port.  This is to
             allow finer resolution of control for high-speed links.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Range: < 0 to 99 >

cost

- interface loopback *< 0 to 7 >* ip ospf *IP-ADDR* cost *< 1 to 65535 >*

```
Set metric of this interface.
```

Range: < 1 to 65535 >

- interface loopback *< 0 to 7 >* ip ospf all cost *< 1 to 65535 >*

```
Set metric of this interface.
```

Range: < 1 to 65535 >

dhcp-snooping

- interface *[ETHERNET] PORT-LIST* dhcp-snooping

```
Usage: [no] dhcp-snooping trust

Description: Configure the port as trusted or untrusted. Only DHCP server
             packets received on trusted interfaces will be forwarded.
             By specifying 'no' the port will be configured as untrusted.
             The default state is untrusted.
```

Next Available Option:

- **trust** -- Configure trusted interfaces**(p. 178)**

direction

- [no] interface *[ETHERNET] PORT-LIST* ip access-group *ACCESS-GROUP < in >*

Supported Values:

- **in** -- Match inbound packets

© 2007 Hewlett-Packard Development Company, L.P.

disable

- interface *[ETHERNET] PORT-LIST* disable

```
Usage: disable

Description: Disable port(s).
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

dscp

- interface *[ETHERNET] PORT-LIST* qos dscp *< 000000 | 000001 | 000010 | ... >*

```
Specify DSCP policy to use.
```

Supported Values:

Binary formatted value from 000000 to 111111

enable

- interface *[ETHERNET] PORT-LIST* enable

```
Usage: enable

Description: Enable port(s).
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

flow-control

- [no] interface *[ETHERNET] PORT-LIST* flow-control

```
Usage: [no] flow-control

Description: Enable/disable flow control on the port(s). By default,
             flow control is disabled. Flow Control is enabled on both
             transmit and receive or auto negotiated if port Mode is set
             to Auto.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

gvrp

- interface *[ETHERNET] PORT-LIST* gvrp

```
Usage: gvrp [join-timer <n>][leave-timer <n>][leaveall-timer <n>]

Description: Set the GVRP timers on the port (hundreths of a second).
             The timers must follow the constraints
             2 * join-timer  <=  leave-timer  <  leaveall-timer
```

Next Available Options:

- **join-timer** < 20 to 75 > -- Set join timer value (centiseconds; default 20).**(p. 167)**
- **leave-timer** < 40 to 300 > -- Set leave timer value (centiseconds; default 300).**(p. 168)**
- **leaveall-timer** < 500 to 3000 > -- Set leaveall timer value (centiseconds; default 1000).**(p. 167)**

© 2007 Hewlett-Packard Development Company, L.P.

icmp

- [no] interface *[ETHERNET] PORT-LIST* rate-limit icmp

```
Set limits for ICMP traffic only.
```

Next Available Option:
- **per-port** < 0 to 100 > -- Specify limit as percent of incoming ICMP traffic.**(p. 172)**

in

- [no] interface *[ETHERNET] PORT-LIST* rate-limit all in

```
Set limits for all inbound traffic.
```

Next Available Options:
- **percent** < 0 to 100 > -- Specify limit as percent of inbound or outbound traffic.**(p. 171)**
- **bps** < 0 to -94967296 > -- Specify limit as bits-per-second of allowed inbound or outbound traffic. (NUMBER) **(p. 163)**

ip

- [no] interface *[ETHERNET] PORT-LIST* ip

```
Usage: [no] ip access-group <ACL-ID> in

Description: Apply the specified access control list to inbound
             packets on this INTERFACE list.  The access
             control list ACL-ID must be defined before it can be applied.
```

Next Available Option:
- **access-group** -- Apply the specified access control list to inbound packets on this INTERFACE list (ASCII-STR) **(p. 160)**

- [no] interface *[ETHERNET] PORT-LIST* monitor ip

```
Apply an IPv4 access list.
```

Next Available Option:
- **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 160)**

- [no] interface loopback *< 0 to 7 >* ip

```
Usage: [no] ip ...

Description: Configure various IP parameters for the Loopback. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
             This is a Loopback context command. It can be called directly
             from the Loopback context or follow the 'interface loopback
             <num>' command.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **address** -- Set IP parameters for communication within an IP network**(p. 161)**
- **ospf** -- configure Open Shortest Path First (OSPF) protocol parameters on the interface**(p. 171)**

ip-addr

- [no] interface loopback *< 0 to 7 >* ip address *IP-ADDR*

```
Interface IP address.
```

- [no] interface loopback *< 0 to 7 >* ip ospf *IP-ADDR*

```
Specify the IP address the request is for.
```

Next Available Options:

- **area** -- Specify an OSPF area.**(p. 162)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 164)**

join-timer

- interface *[ETHERNET] PORT-LIST* gvrp join-timer *< 20 to 75 >*

```
Set join timer value (centiseconds; default 20).
```

Range: < 20 to 75 >

lacp

- [no] interface *[ETHERNET] PORT-LIST* lacp

```
Usage: [no] lacp [active|passive]

Description: Define whether LACP is enabled on the port, and whether it is in
             active or passive mode when enabled.
             When LACP is enabled and active, the port will both send LACP
             packets and listen to them.
             When LACP is enabled and passive, the port will send LACP packets
             only if it is spoken to.
             When LACP is disabled, the port will ignore LACP packets.
             If 'lacp' command is issued without a mode parameter, 'active' is
             assumed.
             With 'no lacp' the mode parameter is not allowed.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Next Available Option:

- **mode** < Active | Passive > -- Define whether LACP is enabled on the port, and whether it is in active or passive mode when enabled**(p. 169)**

leaveall-timer

- interface *[ETHERNET] PORT-LIST* gvrp leaveall-timer *< 500 to 3000 >*

```
Set leaveall timer value (centiseconds; default 1000).
```

Range: < 500 to 3000 >

© 2007 Hewlett-Packard Development Company, L.P.

leave-timer

- interface *[ETHERNET] PORT-LIST* gvrp leave-timer *< 40 to 300 >*

```
Set leave timer value (centiseconds; default 300).
```

Range: < 40 to 300 >

link-keepalive

- [no] interface *[ETHERNET] PORT-LIST* link-keepalive

```
Usage: [no]link-keepalive [vlan <vlan-id>]

Description: Configure UDLD on port(s).
             The command enables/disables UDLD on particular port/port-list
             By default UDLD control packets are untagged.
             The user has to give vlan-id for tagged UDLD control packets.
```

Next Available Option:

- **vlan** -- Set vlan-id for tagged UDLD control packets. (VLAN-ID) **(p. 179)**

loopback

- [no] interface loopback *< 0 to 7 >*

```
Usage: [no] interface loopback <num>

Description: Enter the loopback Configuration Level.
```

Range: < 0 to 7 >

Next Available Option:

- **ip** -- Configure various IP parameters for the Loopback**(p. 166)**

mdix-mode

- interface *[ETHERNET] PORT-LIST* mdix-mode *< mdi | mdix | autoMDIX >*

```
Set port MDI/MDIX mode (default: auto).
```

Supported Values:

- **mdi** -- Configures port for connecting a PC with a crossover cable
- **mdix** -- Configures port for connecting a PC with a straight-through cable
- **autoMDIX** -- Configures port for automatic detection of the cable

mirror

- interface *[ETHERNET] PORT-LIST* monitor all *< In | Out | Both >* mirror

```
Mirror destination.
```

Next Available Options:

- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 170)**
- **mirror_session_name** -- Mirror destination name.**(p. 169)**

- interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP < In >* mirror

© 2007 Hewlett-Packard Development Company, L.P.

```
Mirror destination.
```

Next Available Options:
- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 170)**
- **mirror_session_name** -- Mirror destination name.**(p. 169)**

mirror_session_name

- [no] interface *[ETHERNET] PORT-LIST* monitor all *< In | Out | Both >* mirror

```
Mirror destination name.
```

- [no] interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP < In >* mirror

```
Mirror destination name.
```

mode

- interface *[ETHERNET] PORT-LIST* lacp *< Active | Passive >*

```
Usage: [no] lacp [active|passive]

Description: Define whether LACP is enabled on the port, and whether it is in
             active or passive mode when enabled.
             When LACP is enabled and active, the port will both send LACP
             packets and listen to them.
             When LACP is enabled and passive, the port will send LACP packets
             only if it is spoken to.
             When LACP is disabled, the port will ignore LACP packets.
             If 'lacp' command is issued without a mode parameter, 'active' is
             assumed.
             With 'no lacp' the mode parameter is not allowed.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Supported Values:
- **Active** -- Enable active LACP.
- **Passive** -- Enable passive LACP.

monitor

- [no] interface *[ETHERNET] PORT-LIST* monitor

```
Usage: 1) [no] monitor all <in|out|both> mirror <1-4 | NAME-STR>
               [1-4 | NAME-STR]...
          [no] monitor ip access-group <ACL-NAME> <in> mirror
               <1-4 | NAME-STR> [1-4 | NAME-STR]...

Description: Define either the port is to be monitored or not.
             The network traffic seen by the monitored ports is copied to
             the Mirroring Destination to which a network analyzer can be
             attached.
             Note: When mirroring multiple ports in a busy network,
             some frames may not be copied to the mirroring port.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
Parameters:  o 1-4 - Mirror destination number
             o NAME-STR - Friendly name associated with the mirror
             destination number.
             o ACL-NAME - Standard or Extended Access Control List number.
             o <in|out|both> direction of the traffic to be monitored.
```

Next Available Options:

- **all** < In | Out | Both > -- Monitor all traffic.**(p. 161)**
- **ip** -- Apply an IPv4 access list.**(p. 166)**

monitor_mirror_ACL_dir

- interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP* *< In >*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Supported Values:

- **In** -- Monitor inbound traffic permitted by the ACL

Next Available Option:

- **mirror** -- Mirror destination.**(p. 168)**

monitor_mirror_session_id

- [no] interface *[ETHERNET] PORT-LIST* monitor all *< In | Out | Both >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

- [no] interface *[ETHERNET] PORT-LIST* monitor ip access-group *ACCESS-GROUP* *< In >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

name

- [no] interface *[ETHERNET] PORT-LIST* name

```
Usage:    name PORT-NAME-STR
       no name

Description: Set/unset a name for the port(s).
```

© 2007 Hewlett-Packard Development Company, L.P.

```
This is an Interface context command. It can be called directly
from the interface context or follow the 'interface [ethernet]
PORT-LIST' command.
```

Next Available Option:

- **port-name** -- Specify a port name up to 64 characters length. (ASCII-STR) **(p. 173)**

ospf

- [no] interface loopback *< 0 to 7 >* ip ospf

```
Usage: [no] ip ospf [...]

Description: configure Open Shortest Path First (OSPF)
             protocol parameters on the interface.
             Called without 'no', the command configures OSPF parameter on
             interface. Otherwise ('no' is specified), the command remove
             specified ospf parameter on the interface. Use 'ip ospf ?' to
             get a list of all possible options.
```

Next Available Options:

- **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 167)**
- **all** -- Process the request for all IP addresses.**(p. 161)**

out

- [no] interface *[ETHERNET] PORT-LIST* rate-limit all out

```
Set limits for all outbound traffic.
```

Next Available Options:

- **percent** < 0 to 100 > -- Specify limit as percent of inbound or outbound traffic.**(p. 171)**
- **bps** < 0 to -94967296 > -- Specify limit as bits-per-second of allowed inbound or outbound traffic. (NUMBER) **(p. 163)**

output

- [no] interface *[ETHERNET] PORT-LIST* bandwidth-min output

```
Enable/disable and configure guaranteed minimum bandwidth for outgoing traffic.
```

Next Available Option:

- **queue1** < 0 to 100 > -- Specify min. bandwidth percentage for queue one outgoing traffic.**(p. 174)**

percent

- interface *[ETHERNET] PORT-LIST* rate-limit all in percent *< 0 to 100 >*

```
Specify limit as percent of inbound or outbound traffic.
```

Range: < 0 to 100 >

- interface *[ETHERNET] PORT-LIST* rate-limit all out percent *< 0 to 100 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Specify limit as percent of inbound or outbound traffic.
```

Range: < 0 to 100 >

per-port

- interface *[ETHERNET] PORT-LIST* rate-limit icmp *< 0 to 100 >*

```
Specify limit as percent of incoming ICMP traffic.
```

Range: < 0 to 100 >

port-list

- interface *[ETHERNET] PORT-LIST*

```
Usage: [no] interface [ethernet] PORT-LIST [...]

Description: Enter the Interface Configuration Level, or execute one
             command for that level. Without optional parameters
             specified, the 'interface' command changes the context to
             the Interface Configuration Context Level for execution of
             configuration changes to the port or ports in the PORT-LIST.
             The 'interface [ethernet] PORT-LIST' can be followed by any
             command from the Interface Configuration Context Level in the
             same command line. In this case the context level is not
             changed, but the command is also executed for the port or ports
             in the PORT-LIST. Use 'interface [ethernet] PORT-LIST ?'
             to get a list of all valid commands.
```

Next Available Options:

- **ip** -- Apply the specified access control list to inbound packets on this INTERFACE list**(p. 166)**
- **broadcast-limit** < 0 to 99 > -- Set a broadcast traffic percentage limit**(p. 164)**
- **dhcp-snooping** -- Configure the port as trusted or untrusted**(p. 164)**
- **disable** -- Disable port(s)**(p. 165)**
- **enable** -- Enable port(s)**(p. 165)**
- **flow-control** -- Enable/disable flow control on the port(s)**(p. 165)**
- **gvrp** -- Set the GVRP timers on the port (hundreths of a second)**(p. 165)**
- **lacp** -- Define whether LACP is enabled on the port, and whether it is in active or passive mode when enabled**(p. 167)**
- **mdix-mode** < mdi | mdix | autoMDIX > -- Set port MDI/MDIX mode (default: auto).**(p. 168)**
- **monitor** -- Define either the port is to be monitored or not**(p. 169)**
- **name** -- Set/unset a name for the port(s)**(p. 170)**
- **power** -- Enable/Disable per-port power distribution**(p. 173)**
- **qos** -- Set port-based priority**(p. 173)**
- **speed-duplex** < 10-half | 100-half | 10-full | ... > -- Define mode of operation for the port(s)**(p. 176)**
- **type** < Trunk | | | ... > -- **(p. 178)**
- **unknown-vlans** < Learn | Block | Disable > -- Configure GVRP on the port(s)**(p. 178)**
- **bandwidth-min** -- Enable/disable and configure guaranteed minimum bandwidth settings for outgoing traffic on the port(s)**(p. 163)**
- **rate-limit** -- Enable/disable and configure rate-limiting for all traffic (or for incoming ICMP traffic) on the port(s)**(p. 176)**
- **link-keepalive** -- Configure UDLD on port(s)**(p. 168)**

© 2007 Hewlett-Packard Development Company, L.P.

port-name

- interface *[ETHERNET] PORT-LIST* name *PORT-NAME*

```
Specify a port name up to 64 characters length.
```

power

- [no] interface *[ETHERNET] PORT-LIST* power

```
Usage: [no] power [critical|high|low]

Description: Enable/Disable per-port power distribution. Specifying critical,
             high, or low indicates the priority of the port to get power in
             the event of power over-subscription. Per-port power is enabled
             by default. The default priority is low.
             Note: Lower numbered ports have precedence over higher numbered
             ports of the same priority.
```

Next Available Option:

- **priority** < Critical | High | Low > -- Enable/Disable per-port power distribution**(p. 173)**

priority

- interface *[ETHERNET] PORT-LIST* power *< Critical | High | Low >*

```
Usage: [no] power [critical|high|low]

Description: Enable/Disable per-port power distribution. Specifying critical,
             high, or low indicates the priority of the port to get power in
             the event of power over-subscription. Per-port power is enabled
             by default. The default priority is low.
             Note: Lower numbered ports have precedence over higher numbered
             ports of the same priority.
```

Supported Values:

- **Critical**
- **High**
- **Low**

- interface *[ETHERNET] PORT-LIST* qos priority *< 0 | 1 | 2 | ... >*

```
Specify priority to use.
```

Supported Values:

- **0**
- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**

qos

- [no] interface *[ETHERNET] PORT-LIST* qos

```
Usage: [no] qos [dscp <000000|000001...111111> | priority <0-7>]
```

© 2007 Hewlett-Packard Development Company, L.P.

```
Description: Set port-based priority. The 'dscp' or 'priority' must be
             specified if 'no' is not used. Using 'no' configures the device
             not to apply a source-port priority to this port's packets.
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 165)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 173)**

queue1

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 >*

```
Specify min. bandwidth percentage for queue one outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue2** < 0 to 100 > -- Specify min. bandwidth percentage for queue two outgoing traffic.**(p. 174)**

queue2

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue two outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue3** < 0 to 100 > -- Specify min. bandwidth percentage for queue three outgoing traffic.**(p. 174)**

queue3

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue three outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:

- **queue4** < 0 to 100 > -- Specify min. bandwidth percentage for queue four outgoing traffic.**(p. 174)**

queue4

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue four outgoing traffic.
```

© 2007 Hewlett-Packard Development Company, L.P.

Range: < 0 to 100 >

Next Available Option:
- **queue5** < 0 to 100 > -- Specify min. bandwidth percentage for queue five outgoing traffic.**(p. 175)**

queue5

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue five outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:
- **queue6** < 0 to 100 > -- Specify min. bandwidth percentage for queue six outgoing traffic.**(p. 175)**

queue6

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue six outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:
- **queue7** < 0 to 100 > -- Specify min. bandwidth percentage for queue seven outgoing traffic.**(p. 175)**

queue7

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue seven outgoing traffic.
```

Range: < 0 to 100 >

Next Available Option:
- **queue8** < 0 to 100 > -- Specify min. bandwidth percentage for queue eight outgoing traffic.**(p. 175)**

queue8

- interface *[ETHERNET] PORT-LIST* bandwidth-min output *< 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 > < 0 to 100 >*

```
Specify min. bandwidth percentage for queue eight outgoing traffic.
```

Range: < 0 to 100 >

© 2007 Hewlett-Packard Development Company, L.P.

rate-limit

- interface *[ETHERNET] PORT-LIST* rate-limit

```
Usage: rate-limit <icmp <0-100> | all <in|out> <<0-100> | bps <0-4200000000>>
       no rate-limit <icmp| all <in|out>>>

Description: Enable/disable and configure rate-limiting for all traffic
             (or for incoming ICMP traffic) on the port(s). By default,
             rate-limiting is disabled on all ports. When a port is
             configured to rate-limit traffic, it forwards only that
             specified amount of traffic (percentage or bits-per-second).
             The remaining over-profile traffic of the type being rate-
             limited is then discarded.

             Rate-Limiting works on inbound IGMP traffic, or on inbound or
             outbound traffic in general. The rate-limit reflects the
             permitted forwarding rate of the traffic type. It is visible as
             the average rate of the outbound traffic (or outbound ICMP
             traffic) originating from the rate-limited port (when in inbound
             mode), or as the average rate of the outbound traffic from an
             outbound rate-limited port.

             Rate-limiting of all traffic is primarily used for end-node
             connections (i.e., at the network edge). It is not recommended
             for use on links to servers, routers, switches, or the network
             backbone or core.
             (Rate-limiting all traffic on such links can interfere with
             important network functions.)

             ICMP rate-limiting is primarily used for throttling worm or virus-
             like behavior, and should NOT be used to remove all ICMP traffic
             from the network, as this protocol is necessary for routing
             functions.

             For more detailed information on rate-limiting, please consult
             the product manual.

             This is an Interface context command. It can be called directly
             from the interface context, or following the
             'interface [ethernet] PORT-LIST' command.
```

Next Available Options:

- **icmp** -- Set limits for ICMP traffic only.**(p. 166)**
- **all** -- Set limits for all traffic.**(p. 161)**

speed-duplex

- interface *[ETHERNET] PORT-LIST* speed-duplex *< 10-half | 100-half | 10-full | ... >*

```
Usage: speed-duplex <10-half|100-half|10-full|100-full|1000-full|
                     auto|auto-10|auto-100|auto-1000>

Description: Define mode of operation for the port(s).
             This is an Interface context command. It can be called directly
             from the interface context or follow the 'interface [ethernet]
             PORT-LIST' command.

             For 10FL:
```

© 2007 Hewlett-Packard Development Company, L.P.

```
- 10-half   10 Mbps, half duplex (default). The port operates
            according to the IEEE 802.3/Ethernet standards.
- 10-full   10 Mbps, full duplex. The port simultaneously
            receives and transmits data. (The device attached
            to the port must support full duplex operation).

For 10/100TX:
            Note: Make sure that the device attached to the
            port is configured the same as the selection you
            make here.
- auto      (default) The port automatically selects the
            network speed (10 or 100 Mbps), and that data
            transfer operation (full or half duplex) between
            the switch and another IEEE 802u-compliant device
            running the 'Auto Negotiation' protocol.
- 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-10   Same as 'auto' except that the port speed is fixed
            at 10 Mbps. The data transfer operation (full or
            half duplex) is auto negotiated.

For 100FX:
- 100-full  (default) 100 Mbps, full duplex.
- 100-half  100 Mbps, half duplex.

For 1000T:
- auto      (default) The port automatically selects the
            network speed (100 or 1000 Mbps)and the port
            wiring operation (MDI-X or MDI) between the
            switch and another IEEE 802.3ab-compliant device
            running the 'Auto Negotiation' protocol.
- 100-full  100 Mbps, full duplex.
- auto-100  Same as 'auto'. Limited to 100Mbps network speed.
- auto-1000 Same as 'auto'. Limited to 1000Mbps network speed.

For 1000SX, 1000LX:
- auto      (default) The port Auto Negotiates for Flow
            Control if Flow Control is set to Enable.
- 1000-full 1000 Mbps, full duplex.

For 1000Stk:
- auto      Runs in 1000 Mbps, full duplex.
            The port Auto Negotiates for Flow Control if
            Flow Control is set to Enable.
```

Supported Values:

- **10-half** -- 10 Mbps, half duplex.
- **100-half** -- 100 Mbps, half duplex.
- **10-full** -- 10 Mbps, full duplex.
- **100-full** -- 100 Mbps, full duplex.
- **1000-full** -- 1000 Mbps, full duplex.
- **auto** -- Use Auto Negotiation for speed and duplex mode.
- **auto-10** -- 10 Mbps, use Auto Negotiation for duplex mode.
- **auto-100** -- 100 Mbps, use Auto Negotiation for duplex mode.
- **auto-1000** -- 1000 Mbps, use Auto Negotiation for duplex mode.

© 2007 Hewlett-Packard Development Company, L.P.

trust

- [no] interface *[ETHERNET] PORT-LIST* dhcp-snooping trust

```
Usage: [no] dhcp-snooping trust PORT-LIST

Description: Configure trusted interfaces. Only server packets received
             on trusted interfaces will be forwarded. When 'no' is
             specified the interfaces are marked as untrusted.
             The default port state is untrusted.

Parameters:

    o PORT-LIST - Port list on which to configure trust status.
```

type

- interface *[ETHERNET] PORT-LIST* type *< Trunk | | | ... >*

Supported Values:

- **Trunk**
-
-
- **10FL**
- **10T**
- **10/100TX**
- **100FX**
- **100FX-SFP**
- **Vlan**
- **Mesh**
- **1000SX**
- **1000LX**
- **100/1000T**
- **1000T**
- **1000Stk**
- **1000LH**
- **10GbE-CX4**
- **10GbE-SR**
- **10GbE-ER**
- **10GbE-LR**
- **1000T-SFP**
- **1000X**

unknown-vlans

- interface *[ETHERNET] PORT-LIST* unknown-vlans *< Learn | Block | Disable >*

```
Usage: unknown-vlans <learn|block|disable>

Description: Configure GVRP on the port(s).
             If 'learn' is specified then the port will accept join
             requests for new VLANs on this port and propagate a VLAN
             join requests through all other forwarding ports that are
             participating in GVRP.
             If 'block' is specified then the port will only process
             GRVP packets that concern themselves with known VLANs.
             If 'disable' is specified then all GRVP packets will be
             ignored.
             This is an Interface context command. It can be called directly
```

© 2007 Hewlett-Packard Development Company, L.P.

```
from the interface context or follow the 'interface [ethernet]
PORT-LIST' command.
```

Supported Values:

- **Learn** -- Learn new VLANs.
- **Block** -- Ignore new VLANs.
- **Disable** -- Ignore all GVRP packets.

vlan

- interface *[ETHERNET] PORT-LIST* link-keepalive vlan *VLAN-ID*

```
Set vlan-id for tagged UDLD control packets.
```

© 2007 Hewlett-Packard Development Company, L.P.

ip

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] ip ...

Description: Configure various IP parameters for the switch. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
```

COMMAND STRUCTURE

- [no] ip **access-list** -- Enter the named-acl context for the specified access control list **(p. 182)**
  - **connection-rate-filter** -- Configure a connection-rate-filter Access Control List. **(p. 185)**
    - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 192)**
  - **extended** -- Configure an extended Access Control List. **(p. 188)**
    - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 192)**
    - **number < 100 to 199 >** -- Specify Access Control List to configure by number. **(p. 192)**
  - **resequence** -- Renumber the entries in an Access Control List. **(p. 193)**
    - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 192)**
      - **start-seq-num < 1 to 2147483647 >** -- Specify the starting sequence number. **(p. 196)**
        - **increment < 1 to 2147483646 >** -- Specify the increment. **(p. 190)**
  - **standard** -- Configure a standard Access Control List. **(p. 196)**
    - **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 192)**
    - **number < 1 to 99 >** -- Specify Access Control List to configure by number. **(p. 192)**
- [no] ip **address** -- Set IP parameters for communication within an IP network **(p. 183)**
  - **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters. **(p. 186)**
  - **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 190)**
- [no] ip **arp-age** -- Modify Address Resolution Protocol (ARP) table entry timeout, specified in minutes **(p. 184)**
  - **timeout < 1 to 240 >** -- Modify Address Resolution Protocol (ARP) table entry timeout, specified in minutes (NUMBER) **(p. 196)**
- [no] ip **authorized-managers** -- Define the stations allowed to manage the switch **(p. 184)**
  - **addr** -- Authorized manager IP address. (IP-ADDR) **(p. 183)**
    - **access < Manager | Operator >** -- Define an access level desired. **(p. 182)**
    - **IP-MASK** -- IP mask defining a group of adjacent manager IP addresses. (IP-ADDR) **(p. 191)**
- [no] ip **default-gateway** -- Configure the Layer 2 default gateway address, which will be used when routing is not enabled on the switch **(p. 186)**
  - **ipaddr** -- IP address of the default gateway. (IP-ADDR) **(p. 190)**
- [no] ip **directed-broadcast** -- Enable/disable directed broadcast forwarding **(p. 186)**
- [no] ip **dns** -- Configure the DNS (Domain Name System) default domain suffix and the name server IP address for translation of host names to IP addresses **(p. 187)**
  - **domain-name** -- Configure default domain suffix. **(p. 187)**
    - **domain-name** -- Default domain suffix. (ASCII-STR) **(p. 187)**
  - **server-address** -- Configure DNS server IP address. **(p. 195)**
    - **ipaddr** -- DNS server IP address. (IP-ADDR) **(p. 190)**
- [no] ip **icmp** -- Configure ICMP Rate Limiting capacity **(p. 189)**
  - **addrmask** -- Enable/disable address mask replies **(p. 183)**

© 2007 Hewlett-Packard Development Company, L.P.

- **burst-normal < 0 to 1000000 >** -- The maximum number of icmp replies to send per second **(p. 185)**
- **echo** -- Enable/disable echo replies to broadcast echo requests **(p. 187)**
  - **broadcast-request < Min | Max >** -- Enable/disable echo replies to broadcast echo requests **(p. 185)**
- **redirects** -- Enable/disable redirect error messages **(p. 193)**
- **reply-limit** -- Enable/disable ICMP reply rate limiting **(p. 193)**
- **unreachable** -- Enable/disable destination unreachable error messages **(p. 197)**

■ [no] ip **igmp** -- Enable/disable/configure IP Multicast Group Protocol (IGMP) feature **(p. 189)**
- **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 184)**
- **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 185)**
- **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 188)**
- **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 188)**
- **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 188)**
- **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups **(p. 188)**
- **querier** -- Specify querier/non-querier capability for the VLAN **(p. 193)**

■ [no] ip **irdp** -- Enable/disable ICMP Router Discovery Protocol (IRDP) **(p. 191)**

■ [no] ip **load-sharing** -- Specify the maximum number of equal cost IP load sharing paths **(p. 191)**
- **load-sharing-value < 2 to 4 >** -- Specify the maximum number of equal cost IP load sharing paths **(p. 191)**

■ [no] ip **multicast-routing** -- Enable/disable IP multicast routing on the device **(p. 192)**

■ ip **preserve** -- **(p. 193)**

■ [no] ip **route** -- Add or delete static routing table entries **(p. 193)**
- **ip-addr** -- Specify IP address and mask of the route destination. (IP-ADDR/MASK-LENGTH) **(p. 190)**
  - **blackhole** -- Specify that packets are silently discarded with no ICMP message sent. **(p. 185)**
    - **distance < 1 to 255 >** -- Set the administrative distance to associate with this static route. **(p. 186)**
  - **ip-addr** -- Specify gateway IP address. (IP-ADDR) **(p. 190)**
    - **distance < 1 to 255 >** -- Set the administrative distance to associate with this static route. **(p. 186)**
  - **reject** -- Specify that packets are discarded and ICMP error is returned to sender. **(p. 193)**
    - **distance < 1 to 255 >** -- Set the administrative distance to associate with this static route. **(p. 186)**
  - **vlan** -- Specify the destination VLAN. (VLAN-ID) **(p. 197)**
    - **distance < 1 to 255 >** -- Set the administrative distance to associate with this static route. **(p. 186)**

■ [no] ip **router-id** -- Define the device router id **(p. 194)**
- **ipaddr** -- Define the device router id (IP-ADDR) **(p. 190)**

■ [no] ip **routing** -- Enable/disable IP routing support on the device **(p. 194)**

■ [no] ip **source-binding** -- Add/remove a static IP-to-MAC binding in the DHCP snooping database **(p. 195)**

■ [no] ip **source-route** -- Enable/disable forwarding of source routed packets **(p. 195)**

■ [no] ip **ssh** -- Enable/disable SSH server on the device or set various SSH server parameters **(p. 195)**
- **filetransfer** -- Enable/disable secure file transfer capability. **(p. 188)**
- **port** -- Specify the TCP port on which the daemon should listen for SSH connections. **(p. 192)**
  - **default** -- Specify that the daemon should listen on the default TCP port (22). **(p. 186)**

© 2007 Hewlett-Packard Development Company, L.P.

    - **IP-PORT** -- Specify the TCP port number on which the daemon should listen. (TCP/UDP-PORT) **(p. 191)**
  - **timeout < 5 to 120 >** -- Specify the maximum length of time (seconds) permitted for protocol negotiation and authentication. (NUMBER) **(p. 196)**
- [no] ip **timep** -- Configure the method to acquire the Timep server address **(p. 197)**
  - **dhcp** -- Use DHCP to acquire Timep server address. **(p. 186)**
    - **interval < 1 to 9999 >** -- Specify how often (in minutes) the switch tries to get the current time. **(p. 190)**
  - **manual** -- Manually configure the Timep server address. **(p. 191)**
    - **interval < 1 to 9999 >** -- Specify how often (in minutes) the switch tries to get the current time. **(p. 190)**
    - **server** -- Timep server IP address. (IP-ADDR) **(p. 194)**
- ip **ttl < 2 to 255 >** -- Specify TTL for outgoing IP packets (NUMBER) **(p. 197)**
- [no] ip **udp-bcast-forward** -- Enable/disable UDP broadcast forwarding **(p. 197)**
- [no] ip **zero-broadcast** -- Enable/disable usage of zero broadcast IP Address **(p. 198)**

COMMAND DETAILS

access (p. 182)
access-list (p. 182)
addr (p. 183)
address (p. 183)
addrmask (p. 183)
arp-age (p. 184)
authorized-managers (p. 184)
auto (p. 184)
blackhole (p. 185)
blocked (p. 185)
broadcast-request (p. 185)
burst-normal (p. 185)
connection-rate-filter (p. 185)
default (p. 186)
default-gateway (p. 186)
dhcp (p. 186)
dhcp-bootp (p. 186)
directed-broadcast (p. 186)
distance (p. 186)
dns (p. 187)
domain-name (p. 187)
echo (p. 187)
extended (p. 188)
fastleave (p. 188)
filetransfer (p. 188)
forcedfastleave (p. 188)
forward (p. 188)
high-priority-forward (p. 188)
icmp (p. 189)
igmp (p. 189)
increment (p. 190)
interval (p. 190)
ipaddr (p. 190)
ip-addr (p. 190)
IP-MASK (p. 191)
IP-PORT (p. 191)
irdp (p. 191)
load-sharing (p. 191)
load-sharing-value (p. 191)
manual (p. 191)
multicast-routing (p. 192)
name (p. 192)
number (p. 192)
port (p. 192)
preserve (p. 193)
querier (p. 193)
redirects (p. 193)
reject (p. 193)
reply-limit (p. 193)
resequence (p. 193)
route (p. 193)
router-id (p. 194)
routing (p. 194)
server (p. 194)
server-address (p. 195)
source-binding (p. 195)
source-route (p. 195)
ssh (p. 195)
standard (p. 196)
start-seq-num (p. 196)
timeout (p. 196)
timep (p. 197)
ttl (p. 197)
udp-bcast-forward (p. 197)
unreachable (p. 197)
vlan (p. 197)
zero-broadcast (p. 198)

access

- ip authorized-managers *IP-ADDR* access *< Manager | Operator >*

```
Define an access level desired.
```

Supported Values:
- **Manager**
- **Operator**

access-list

- [no] ip access-list

```
Usage: [no] ip access-list <extended|standard|conection-rate-filter> <ACL-ID>

Description: Enter the named-acl context for the specified access control
             list.  The ACL-ID is case sensitive and may be up to sixty-four
             characters in length.  If it includes spaces, the entire ACL-ID
             must be enclosed in quotation marks.
```

Next Available Options:

- **extended** -- Configure an extended Access Control List. **(p. 188)**
- **standard** -- Configure a standard Access Control List. **(p. 196)**
- **resequence** -- Renumber the entries in an Access Control List. **(p. 193)**
- **connection-rate-filter** -- Configure a connection-rate-filter Access Control List. **(p. 185)**

See the access-list command for extended, standard, and connection-rate-filter command syntax information.(p. 53)

addr

- ip authorized-managers *IP-ADDR*

```
Authorized manager IP address.
```

Next Available Options:

- **IP-MASK** -- IP mask defining a group of adjacent manager IP addresses. (IP-ADDR) **(p. 191)**
- **access** < Manager | Operator > -- Define an access level desired.**(p. 182)**

address

- [no] ip address

```
Usage: [no] ip address [dhcp-bootp|IP-ADDR/MASK-LENGTH]

Description: Set IP parameters for communication within an IP network.

Parameters:

    o dhcp-bootp - The switch attempts to get its configuration from a
      DHCP/Bootp server.

    o IP-ADDR/MASK-LENGTH - Assign an IP address to the switch.
      The IP-ADDR/MASK-LENGTH may be specified in two ways using the
      following syntax:
          ip address 192.32.36.87/24
          ip address 192.32.36.87 255.255.255.0
      Both of the statements above would have the same effect.
```

Next Available Options:

- **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 190)**
- **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters.**(p. 186)**

addrmask

- [no] ip icmp addrmask

```
Usage: [no] ip icmp addrmask

Description: Enable/disable address mask replies.
```

© 2007 Hewlett-Packard Development Company, L.P.

arp-age

- [no] ip arp-age

```
Usage: ip arp-age <1..240>

Description: Modify Address Resolution Protocol (ARP) table entry timeout,
             specified in minutes.
             The default timeout is 20 minutes.
```

Next Available Option:

- **timeout** < 1 to 240 > -- Modify Address Resolution Protocol (ARP) table entry timeout, specified in minutes (NUMBER) **(p. 196)**

authorized-managers

- [no] ip authorized-managers

```
Usage: [no] ip authorized-managers <IP-ADDR [IP-MASK]>
               access [manager|operator] [IP-MASK]

Description: Define the stations allowed to manage the switch.
             The stations specified are allowed to access the
             switch's Web browser interface, to telnet to the switch
             and to perform TFTP operations.
             A maximum of 10 addresses may be configured.

Parameters:

    o IP-ADDR - The IP address of an authorized manager.

    o IP-MASK - A mask that allows you to define which portions of
      the listed IP address need to be matched by an incoming request.
      The default mask is 255.255.255.255. For example, with an
      authorized address of 10.8.11.1 and a mask of 255.255.255.255,
      only access from 10.8.11.1 is allowed. With a mask of
      255.255.255.0, access from any IP address with 10.8.11.x is
      allowed.

    o [manager|operator] - A designation of the management capabilities
      that are accessible to the authorized manager.
      'manager' allows full access to all web browser and telnet to console
      for viewing and setting the switch configuration, and for performing
      all other interface operations,including all TFTP operations.
      'operator' allows view-only access from the web browser and the
      console,but does not allow changing the switch configuration or any
      TFTP operations.The default access level is manager.
```

Next Available Option:

- **addr** -- Authorized manager IP address. (IP-ADDR) **(p. 183)**

auto

- ip igmp auto *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp auto [ethernet] PORT-LIST

Description: Instruct the device to monitor incoming multicast traffic
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                on the specified ports (this is the default behavior).  This
                feature is configured on a per-VLAN basis.
```

blackhole

- [no] ip route *IP-ADDR/MASK-LENGTH* blackhole

```
Specify that packets are silently discarded with no ICMP message sent.
```

Next Available Option:

- **distance** < 1 to 255 > -- Set the administrative distance to associate with this static route.**(p. 186)**

blocked

- ip igmp blocked *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp block [ethernet] PORT-LIST

Description: Instruct the device to drop incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

broadcast-request

- [no] ip icmp echo broadcast-request

```
Usage: [no] ip icmp echo broadcast-request

Description: Enable/disable echo replies to broadcast echo requests.
```

Supported Values:

- **Min**
- **Max**

burst-normal

- [no] ip icmp burst-normal *< 0 to 1000000 >*

```
Usage: ip icmp burst-normal <0-1000000>

Description: The maximum number of icmp replies to send per second.
             The default value is 1000.
```

Range: < 0 to 1000000 >

connection-rate-filter

- [no] ip access-list connection-rate-filter

```
Configure a connection-rate-filter Access Control List.
```

See the access-list command for extended, standard, and connection-rate-filter command syntax information.(p. 53)

Next Available Option:

- **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 192)**

© 2007 Hewlett-Packard Development Company, L.P.

default

- ip ssh port default

```
Specify that the daemon should listen on the default TCP port (22).
```

default-gateway

- [no] ip default-gateway

```
Usage: [no] ip default-gateway [IP-ADDR]

Description: Configure the Layer 2 default gateway address, which will be
             used when routing is not enabled on the switch. The IP-ADDR
             must be specified if the command is not preceded by 'no'.
             Preceding the command with 'no' deletes the default gateway
             address.
```

Next Available Option:

- **ipaddr** -- IP address of the default gateway. (IP-ADDR) **(p. 190)**

dhcp

- ip timep dhcp

```
Use DHCP to acquire Timep server address.
```

Next Available Option:

- **interval** < 1 to 9999 > -- Specify how often (in minutes) the switch tries to get the current time.**(p. 190)**

dhcp-bootp

- ip address dhcp-bootp

```
Configure the interface to use DHCP/Bootp server to acquire parameters.
```

directed-broadcast

- [no] ip directed-broadcast

```
Usage: [no] ip directed-broadcast

Description: Enable/disable directed broadcast forwarding.
```

distance

- ip route *IP-ADDR/MASK-LENGTH IP-ADDR* distance *< 1 to 255 >*

```
Set the administrative distance to associate with this static route.
```

Range: < 1 to 255 >

- ip route *IP-ADDR/MASK-LENGTH* vlan *VLAN-ID* distance *< 1 to 255 >*

```
Set the administrative distance to associate with this static route.
```

Range: < 1 to 255 >

- ip route *IP-ADDR/MASK-LENGTH* reject distance *< 1 to 255 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Set the administrative distance to associate with this static route.
```

Range: < 1 to 255 >

- ip route *IP-ADDR/MASK-LENGTH* blackhole distance *< 1 to 255 >*

```
Set the administrative distance to associate with this static route.
```

Range: < 1 to 255 >

dns

- [no] ip dns

```
Usage: [no] ip dns [domain-name <domain-name> | server-address <IP-ADDR>]

Description: Configure the DNS (Domain Name System) default domain suffix
             and the name server IP address for translation of host names
             to IP addresses.

             No additional parameters required when 'no' is specified.

Parameters:
    o domain-name <domain-name> - The default domain suffix.

    o server-address <IP-ADDR>  - The IP address of the DNS name server.
```

Next Available Options:

- **domain-name** -- Configure default domain suffix.**(p. 187)**
- **server-address** -- Configure DNS server IP address.**(p. 195)**

domain-name

- [no] ip dns domain-name

```
Configure default domain suffix.
```

Next Available Option:

- **domain-name** -- Default domain suffix. (ASCII-STR) **(p. 187)**

- ip dns domain-name *DOMAIN-NAME*

```
Default domain suffix.
```

echo

- [no] ip icmp echo

```
Usage: [no] ip icmp echo ...

Description: Enable/disable echo replies to broadcast echo requests.
```

Next Available Option:

- **broadcast-request** < Min | Max > -- Enable/disable echo replies to broadcast echo requests**(p. 185)**

© 2007 Hewlett-Packard Development Company, L.P.

extended

- [no] ip access-list extended

```
Configure an extended Access Control List.
```

See the access-list command for extended, standard, and connection-rate-filter command syntax information.(p. 53)

Next Available Options:

- **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 192)**
- **number** < 100 to 199 > -- Specify Access Control List to configure by number. **(p. 192)**

fastleave

- [no] ip igmp fastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp fastleave [ethernet] PORT-LIST

Description: Enables or disables IGMP Fast Leaves. When enabled, as soon as
             an IGMP Group Leave has been received on a non-cascaded port,
             the switch stops forwarding multicast traffic for that group
             to that port.
             Does not apply to cascaded ports (see ip igmp forcedfastleave).
             When disabled, or when the port is cascaded, the regular IGMP
             leave time is used (up to 10 seconds when the switch is not
             the IGMP Querier).
             The default behavior is for IGMP FastLeaves to be enabled.
             This feature is configured for ports on a per-VLAN basis.
```

filetransfer

- [no] ip ssh filetransfer

```
Enable/disable secure file transfer capability.
```

forcedfastleave

- [no] ip igmp forcedfastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp forcedfastleave [ethernet] PORT-LIST

Description: When enabled, this feature forces IGMP Fast Leaves to occur
             even when the port is cascaded. See 'ip igmp fastleave' for
             more information.  The default behavior is for IGMP Forced
             FastLeaves to be disabled.
             This feature is configured for ports on a per-VLAN basis.
```

forward

- ip igmp forward *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp forward [ethernet] PORT-LIST

Description: Instruct the device to forward incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

high-priority-forward

- [no] ip igmp high-priority-forward

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] ip igmp high-priority-forward

Description: Enable/disable the high priority forwarding of traffic for
             subscribed IP Multicast groups. This feature is configured on
             a per-VLAN  basis.
```

icmp

- [no] ip icmp

```
Usage: [no] ip icmp [...]

Description: Configure ICMP Rate Limiting capacity. Use 'ip icmp ?' to get
             a list of all possible configurable parameters.
```

Next Available Options:

- **addrmask** -- Enable/disable address mask replies**(p. 183)**
- **burst-normal** < 0 to 1000000 > -- The maximum number of icmp replies to send per second**(p. 185)**
- **echo** -- Enable/disable echo replies to broadcast echo requests**(p. 187)**
- **redirects** -- Enable/disable redirect error messages**(p. 193)**
- **reply-limit** -- Enable/disable ICMP reply rate limiting**(p. 193)**
- **unreachable** -- Enable/disable destination unreachable error messages**(p. 197)**

igmp

- [no] ip igmp

```
Usage: [no] ip igmp [...]

Description: Enable/disable/configure IP Multicast Group Protocol (IGMP)
             feature.  This command enables, disables or configures the
             IGMP feature for IGMP communication between Multicast
             Routers, Multicast Servers, and Multicast Clients connected
             to the switch.  If not preceded by 'no', the command accepts
             a variety of configuration parameters. To get a list of all
             available parameters use 'ip igmp ?'. To get a detailed help
             for a parameter, follow it with 'help' keyword.
```

Next Available Options:

- **querier** -- Specify querier/non-querier capability for the VLAN**(p. 193)**
- **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups**(p. 188)**
- **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 184)**
- **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 185)**
- **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 188)**
- **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 188)**
- **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 188)**

© 2007 Hewlett-Packard Development Company, L.P.

increment

- ip access-list resequence *NAME < 1 to 2147483647 > < 1 to 2147483646 >*

```
Specify the increment.
```

Range: < 1 to 2147483646 >

interval

- ip timep dhcp interval *< 1 to 9999 >*

```
Specify how often (in minutes) the switch tries to get the current time.
```

Range: < 1 to 9999 >

- ip timep manual interval *< 1 to 9999 >*

```
Specify how often (in minutes) the switch tries to get the current time.
```

Range: < 1 to 9999 >

ipaddr

- ip default-gateway *IP-ADDR*

```
IP address of the default gateway.
```

- ip dns server-address *IP-ADDR*

```
DNS server IP address.
```

- ip router-id *IP-ADDR*

```
Usage: ip router-id IP-ADDR
       [no] ip router-id

Description: Define the device router id.
             The no form of the command clears the router-id.
```

ip-addr

- [no] ip address *IP-ADDR/MASK-LENGTH*

```
Interface IP address/mask.
```

- ip route *IP-ADDR/MASK-LENGTH*

```
Specify IP address and mask of the route destination.
```

Next Available Options:

- **ip-addr** -- Specify gateway IP address. (IP-ADDR) **(p. 190)**
- **vlan** -- Specify the destination VLAN. (VLAN-ID) **(p. 197)**
- **reject** -- Specify that packets are discarded and ICMP error is returned to sender.**(p. 193)**
- **blackhole** -- Specify that packets are silently discarded with no ICMP message sent.**(p. 185)**

- [no] ip route *IP-ADDR/MASK-LENGTH IP-ADDR*

```
Specify gateway IP address.
```

Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **distance** < 1 to 255 > -- Set the administrative distance to associate with this static route.**(p. 186)**

IP-MASK

- ip authorized-managers *IP-ADDR IP-ADDR*

```
IP mask defining a group of adjacent manager IP addresses.
```

IP-PORT

- ip ssh port *TCP/UDP-PORT*

```
Specify the TCP port number on which the daemon should listen.
```

irdp

- [no] ip irdp

```
Usage: [no] ip irdp

Description: Enable/disable ICMP Router Discovery Protocol (IRDP).
             To configure IRDP, execute '[no] ip irdp [...]' from the
             VLAN context for the VLAN on which you wish to configure IRDP.
```

load-sharing

- [no] ip load-sharing

```
Usage: ip load-sharing <2-4>
       no ip load-sharing

Description: Specify the maximum number of equal cost IP load sharing
             paths.  no ip load-sharing disables IP load sharing.
```

Next Available Option:

- **load-sharing-value** < 2 to 4 > -- Specify the maximum number of equal cost IP load sharing paths**(p. 191)**

load-sharing-value

- ip load-sharing *< 2 to 4 >*

```
Usage: ip load-sharing <2-4>
       no ip load-sharing

Description: Specify the maximum number of equal cost IP load sharing
             paths.  no ip load-sharing disables IP load sharing.
```

Range: < 2 to 4 >

manual

- ip timep manual

```
Manually configure the Timep server address.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **server** -- Timep server IP address. (IP-ADDR) **(p. 194)**
- **interval** < 1 to 9999 > -- Specify how often (in minutes) the switch tries to get the current time.**(p. 190)**

multicast-routing

- [no] ip multicast-routing

```
Usage: [no] ip multicast-routing

Description: Enable/disable IP multicast routing on the device.
```

name

- [no] ip access-list extended *NAME*

```
Specify name of Access Control List to configure.
```

- [no] ip access-list standard *NAME*

```
Specify name of Access Control List to configure.
```

- ip access-list resequence *NAME*

```
Specify name of Access Control List to configure.
```

Next Available Option:

- **start-seq-num** < 1 to 2147483647 > -- Specify the starting sequence number. **(p. 196)**

- [no] ip access-list connection-rate-filter *NAME*

```
Specify name of Access Control List to configure.
```

number

- [no] ip access-list extended *< 100 to 199 >*

```
Specify Access Control List to configure by number.
```

Range: < 100 to 199 >

- [no] ip access-list standard *< 1 to 99 >*

```
Specify Access Control List to configure by number.
```

Range: < 1 to 99 >

port

- ip ssh port

```
Specify the TCP port on which the daemon should listen for SSH connections.
```

Next Available Options:

- **IP-PORT** -- Specify the TCP port number on which the daemon should listen. (TCP/UDP-PORT) **(p. 191)**
- **default** -- Specify that the daemon should listen on the default TCP port (22).**(p. 186)**

© 2007 Hewlett-Packard Development Company, L.P.

preserve

- ip preserve

querier

- [no] ip igmp querier

```
Usage: [no] ip igmp querier

Description: Specify querier/non-querier capability for the VLAN. IGMP
             queries are not sent when the mode is disabled. When
             enabled, the device cannot become Querier for the subnet
             unless the VLAN has an IP Address (use the 'show ip' command
             to determine this).  Each subnet must have at least one IGMP
             Querier-capable device in order for IGMP to function
             properly.
```

redirects

- [no] ip icmp redirects

```
Usage: [no] ip icmp redirects

Description: Enable/disable redirect error messages.
```

reject

- [no] ip route *IP-ADDR/MASK-LENGTH* reject

```
Specify that packets are discarded and ICMP error is returned to sender.
```

Next Available Option:

- **distance** < 1 to 255 > -- Set the administrative distance to associate with this static route.**(p. 186)**

reply-limit

- [no] ip icmp reply-limit

```
Usage: ip icmp reply-limit

Description: Enable/disable ICMP reply rate limiting.
```

resequence

- ip access-list resequence

```
Renumber the entries in an Access Control List.
```

Next Available Option:

- **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 192)**

route

- [no] ip route

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] ip route IP-ADDR/MASK-LENGTH
             <IP-ADDR|vlan <vlan-id>|reject|blackhole> [distance <1-255>]

Description: Add or delete static routing table entries. A route
             entry is identified by a destination (IP-ADDR/MASK-LENGTH)
             and next-hop pair. The next-hop can be either a gateway IP
             address or a vlan or the keyword 'reject' or 'blackhole':
             - a gateway IP address indicates that the specified gateway
               will be used to reach the destination. The gateway address is
               not required to be directly reachable on one of local subnets.
               If the gateway address is not directly reachable, the route
               will be added to the routing table as soon as a route to the
               gateway address is learned.
               If the gateway address is one of local interface addresses,
               the destination is treated as if it is directly connected to
               the specified interface.
             - the keyword 'vlan' followed by the vlan-id indicates the
               destination vlan for that route.
             - the keyword 'reject' indicates that if this route is matched,
               a packet to the destination is discarded and a notification
               (e.g. ICMP error) is returned to the packet sender.
             - the keyword 'blackhole' indicates that if this route is matched,
               a packet to the destination is silently discarded and no
               notification (e.g. ICMP error) is returned to the packet sender.
             - the optional keyword 'distance' is used to specify the
               administrative distance for the route.
             If the route command is preceded by 'no' the command deletes
             the route for the specified destination next-hop pair.
```

Next Available Option:

- **ip-addr** -- Specify IP address and mask of the route destination. (IP-ADDR/MASK-LENGTH) **(p. 190)**

router-id

- [no] ip router-id

```
Usage: ip router-id IP-ADDR
       [no] ip router-id

Description: Define the device router id.
             The no form of the command clears the router-id.
```

Next Available Option:

- **ipaddr** -- Define the device router id (IP-ADDR) **(p. 190)**

routing

- [no] ip routing

```
Usage: [no] ip routing

Description: Enable/disable IP routing support on the device.
```

server

- ip timep manual *IP-ADDR*

© 2007 Hewlett-Packard Development Company, L.P.

```
Timep server IP address.
```

server-address

- [no] ip dns server-address

```
Configure DNS server IP address.
```

Next Available Option:

- (p. 190) -- DNS server IP address. (IP-ADDR) (p. 190)

source-binding

- [no] ip source-binding <VLAN-ID><MAC-ADDR><IP-ADDR>[ethernet]<PORT-NUM>

```
Add/remove a static IP-to-MAC binding in the DHCP snooping database.
Parameters:
            o  VLAN-ID - VLAN-ID number to bind with the specified IP and
               MAC address on the specified port in the DHCP snooping
               binding database.
            o  MAC-ADDR - MAC address to bind with the specified IP
               address and VLAN on the specified port.
            o  IP-ADDR - IP address to bind with the specified MAC
               address and VLAN on the specified port.
            o  [ethernet]PORT-NUM - Port number on which the IP-to-MAC and
               VLAN binding is configured on.
```

source-route

- [no] ip source-route

```
Usage: [no] ip source-route

Description: Enable/disable forwarding of source routed packets.
```

Caution

Source routing is enabled by default on the switch and can be used to override ACLs. For this reason, if you are using ACLs to enhance network security, the recommended action is to use the "no ip source-route" command to disable source routing on the switch. (If source routing is disabled in the running-config file, the "show running-config" (p. 378) command includes "no ip source-route" in the running-config file listing.)

ssh

- [no] ip ssh

```
Usage: ip ssh filetransfer
              port <<1-65535>|default>
              timeout <5-120>
       no ip ssh [filetransfer]

Description: Enable/disable SSH server on the device or set various SSH
             server parameters.

Parameters:

           o 'filetransfer' - Enable/disable secure file transfer
             capability.  Secure file transfer will not function unless
```

```
    SSH is also enabled.

  o 'port <<1-65535>|default>' - Set the TCP port on which the
    daemon should listen for SSH connections. The default is 22.

  o 'timeout <5-120>' - Set the maximum length of time in
    seconds permitted for initial protocol negotiation and
    authentication. The default is 120 seconds.
```

Next Available Options:
- **filetransfer** -- Enable/disable secure file transfer capability.**(p. 188)**
- **port** -- Specify the TCP port on which the daemon should listen for SSH connections.**(p. 192)**
- **timeout** < 5 to 120 > -- Specify the maximum length of time (seconds) permitted for protocol negotiation and authentication. (NUMBER) **(p. 196)**

standard

- [no] ip access-list standard

```
Configure a standard Access Control List.
```

See the access-list command for extended, standard, and connection-rate-filter command syntax information.(p. 53)

Next Available Options:
- **name** -- Specify name of Access Control List to configure. (ASCII-STR) **(p. 192)**
- **number** < 1 to 99 > -- Specify Access Control List to configure by number. **(p. 192)**

start-seq-num

- ip access-list resequence *NAME < 1 to 2147483647 >*

```
Specify the starting sequence number.
```

Range: < 1 to 2147483647 >

Next Available Option:
- **increment** < 1 to 2147483646 > -- Specify the increment. **(p. 190)**

timeout

- ip arp-age *< 1 to 240 >*

```
Usage: ip arp-age <1..240>

Description: Modify Address Resolution Protocol (ARP) table entry timeout,
             specified in minutes.
             The default timeout is 20 minutes.
```

Range: < 1 to 240 >

- ip ssh timeout *< 5 to 120 >*

```
Specify the maximum length of time (seconds) permitted for protocol negotiation and
authentication.
```

Range: < 5 to 120 >

© 2007 Hewlett-Packard Development Company, L.P.

timep

- [no] ip timep

```
Usage: [no] ip timep [<dhcp|manual IP-ADDR> [interval <1-9999>]]


Description: Configure the method to acquire the Timep server address.
             No additional parameters required when 'no' is specified.

Parameters:

    o <dhcp|manual> - The method the switch uses to acquire
      the Timep server address: dhcp - from a DHCP server; manual - you
      manually enter the Timep server address; disable (which is set by
      specifying the 'no' parameter) - the switch will not attempt to get
      its time from a Timep server.

    o [interval <1-9999>] (default is 720) How often (in minutes) the
      switch tries to get the current time.

    o [server <IP-ADDR>] - The IP address of the Timep server that the
      switch gets the current time from.
```

Next Available Options:

- **dhcp** -- Use DHCP to acquire Timep server address.**(p. 186)**
- **manual** -- Manually configure the Timep server address.**(p. 191)**

ttl

- ip ttl *< 2 to 255 >*

```
Usage: ip ttl <2-255>

Description: Specify TTL for outgoing IP packets.
```

Range: < 2 to 255 >

udp-bcast-forward

- [no] ip udp-bcast-forward

```
Usage: [no] ip udp-bcast-forward

Description: Enable/disable UDP broadcast forwarding.
```

unreachable

- [no] ip icmp unreachable

```
Usage: [no] ip icmp unreachable

Description: Enable/disable destination unreachable error messages.
```

vlan

- [no] ip route *IP-ADDR/MASK-LENGTH* vlan *VLAN-ID*

```
Specify the destination VLAN.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:

- **distance** < 1 to 255 > -- Set the administrative distance to associate with this static route.**(p. 186)**

zero-broadcast

- [no] ip zero-broadcast

```
Usage: [no] ip zero-broadcast

Description: Enable/disable usage of zero broadcast IP Address.
```

© 2007 Hewlett-Packard Development Company, L.P.

key-chain

OVERVIEW

Category:	Switch Security
Primary context:	config
Related Commands	**show key-chain (page 360)**

```
Usage: key-chain ASCII-STR
Usage: key-chain ASCII-STR key NUMBER [key-string ASCII-STR]
       [accept-lifetime <infinite|<<START-TIME|now> <END-TIME|duration SEC>>>]
       [send-lifetime <infinite|<<START-TIME|now> <END-TIME|duration SEC>>>]
Usage: no key-chain ASCII-STR
Usage: no key-chain ASCII-STR key KEY-ID

Description: Configures authentication key chains and individual keys.
             The configured key chains can be used for routing protocol
             authentication. Refer to routing protocol configuration
             commands for supported authentication methods and further
             instructions. The first form of command creates a new key
             chain unless the identified chain already exists.
             The second form of the command allows adding keys to an
             existent chain. The third and fourth forms of the command
             can be used to delete keys and chains.
             Parameters:
             - 'key-string ASCII-STR' authentication key to use
                (default empty string).
             - 'accept-lifetime ...' time and date when to start accepting
                the key and when the key is going to expire. The
                expiration time is set to 'infinite' by default.
             - 'send-lifetime ...' time and date when to start using
                the key to send and when the key is going to expire.
                A send key is always an accept key too. The expiration
                time is set to 'infinite' by default.
             Note: The 'accept-lifetime' period must always include the
             'send-lifetime' period. If only one of the periods is being
             changed then the other period also will be increased/reduced
             when it is necessary.
             Note: All time values are assumed to be GMT
```

COMMAND STRUCTURE

- [no] key-chain KEY-CHAIN **key < 0 to 255 >** -- Configure chain keys. (NUMBER) **(p. 213)**
  - **accept-lifetime** -- Set key accept lifetime. **(p. 203)**
    - **date** -- Key accept start date. (MM/DD[/[YY]YY]) **(p. 203)**
      - **time** -- Key accept start time. (HH:MM[:SS]) **(p. 218)**
        - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 203)**
          - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
            - **send-lifetime** -- Set key send lifetime. **(p. 216)**
              - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
                - *additional options available...*
              - **infinite** -- Set infinite lifetime. **(p. 212)**
              - **now** -- Use current day and time. **(p. 214)**
                - *additional options available...*
        - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

© 2007 Hewlett-Packard Development Company, L.P.

- **send-lifetime** -- Set key send lifetime. **(p. 216)**
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
    - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**
      - *additional options available...*
  - **infinite** -- Set infinite lifetime. **(p. 212)**
  - **now** -- Use current day and time. **(p. 214)**
    - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
      - *additional options available...*
    - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
- **infinite** -- Set infinite lifetime. **(p. 212)**
  - **send-lifetime** -- Set key send lifetime. **(p. 216)**
    - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
      - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**
        - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
          - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
        - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
    - **infinite** -- Set infinite lifetime. **(p. 212)**
    - **now** -- Use current day and time. **(p. 214)**
      - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
        - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
      - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
- **now** -- Use current day and time. **(p. 214)**
  - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 203)**
    - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
      - **send-lifetime** -- Set key send lifetime. **(p. 216)**
        - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
          - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**
            - *additional options available...*
        - **infinite** -- Set infinite lifetime. **(p. 212)**
        - **now** -- Use current day and time. **(p. 214)**
          - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
            - *additional options available...*
          - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
    - **send-lifetime** -- Set key send lifetime. **(p. 216)**
      - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
        - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**
          - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
            - *additional options available...*
          - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
      - **infinite** -- Set infinite lifetime. **(p. 212)**
      - **now** -- Use current day and time. **(p. 214)**
        - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
          - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
        - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
- **key-string** -- Set key string (ASCII-STR) **(p. 214)**
  - **accept-lifetime** -- Set key accept lifetime. **(p. 203)**
    - **date** -- Key accept start date. (MM/DD[/[YY]YY]) **(p. 203)**
      - **time** -- Key accept start time. (HH:MM[:SS]) **(p. 218)**
        - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 203)**
          - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
            - **send-lifetime** -- Set key send lifetime. **(p. 216)**
              - *additional options available...*

© 2007 Hewlett-Packard Development Company, L.P.

- **duration** -- Use current day and time. (NUMBER) **(p. 210)**
  - **send-lifetime** -- Set key send lifetime. **(p. 216)**
    - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
      - *additional options available...*
    - **infinite** -- Set infinite lifetime. **(p. 212)**
    - **now** -- Use current day and time. **(p. 214)**
      - *additional options available...*
- **infinite** -- Set infinite lifetime. **(p. 212)**
  - **send-lifetime** -- Set key send lifetime. **(p. 216)**
    - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
      - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**
        - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
          - *additional options available...*
        - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
    - **infinite** -- Set infinite lifetime. **(p. 212)**
    - **now** -- Use current day and time. **(p. 214)**
      - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
        - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
      - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
- **now** -- Use current day and time. **(p. 214)**
  - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 203)**
    - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
      - **send-lifetime** -- Set key send lifetime. **(p. 216)**
        - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
          - *additional options available...*
        - **infinite** -- Set infinite lifetime. **(p. 212)**
        - **now** -- Use current day and time. **(p. 214)**
          - *additional options available...*
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
    - **send-lifetime** -- Set key send lifetime. **(p. 216)**
      - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
        - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**
          - *additional options available...*
      - **infinite** -- Set infinite lifetime. **(p. 212)**
      - **now** -- Use current day and time. **(p. 214)**
        - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
          - *additional options available...*
        - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- **send-lifetime** -- Set key send lifetime. **(p. 216)**
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
    - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**
      - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
        - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
      - **duration** -- Use current day and time. (NUMBER) **(p. 210)**
  - **infinite** -- Set infinite lifetime. **(p. 212)**
  - **now** -- Use current day and time. **(p. 214)**
    - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
      - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
    - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- **send-lifetime** -- Set key send lifetime. **(p. 216)**
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
    - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**
      - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**

- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- **infinite** -- Set infinite lifetime. **(p. 212)**
- **now** -- Use current day and time. **(p. 214)**
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

EXAMPLES

Example: key-chain

Generate a new key chain entry:

```
HP Switch(config)# key-chain Procurve1
HP Switch(config)# show key-chain

 Key Chains

  Chain Name                       Keys Active Expired
  -------------------------------- ---- ------ -------
  Procurve1                        0    0      0
```

Example: key-chain key

Generate a new time-independent key for the Procurve1 key chain entry:

```
HP Switch(config)# key-chain Procurve1 key 1
HP Switch(config)# show key-chain Procurve1

 Chain - Procurve1

  Key | Accept Start GMT  Accept Stop GMT   Send Start GMT    Send Stop GMT
  --- + ----------------- ----------------- ----------------- -----------------
  1   | Bootup            Infinite          Bootup            Infinite

  OSPF Interface References

  Interface
  ---------------

  OSPF Virtual Link References

  Area/Virtual Link
  ------------------------------
```

Example: key-chain key accept-lifetime

Add some keys to the key chain entry "Procurve2":

```
HP Switch(config)# key-chain Procurve2 key 1 accept-lifetime 01/17/03 8:00:00
01/18/03 8:10:00 send-lifetime 01/17/03 8:00:00 01/18/03 8:00:00
HP Switch(config)# key-chain Procurve2 key 2 accept-lifetime 01/18/03 8:00:00
duration 87000 send-lifetime 01/18/03 8:00:00 duration 86400
HP Switch(config)# key-chain Procurve2 key 3 accept-lifetime 01/19/03 8:00:00
duration 87000 send-lifetime 01/19/03 8:00:00 duration 86400
HP Switch(config)# key-chain Procurve2 key 4 accept-lifetime 01/20/03 8:00:00
duration 87000 send-lifetime 01/20/03 8:00:00 duration 86400
HP Switch(config)# key-chain Procurve2 key 5 accept-lifetime 01/21/03 8:00:00
duration 87000 send-lifetime 01/21/03 8:00:00 duration 86400
```

COMMAND DETAILS

accept-lifetime (p. 203)	**infinite (p. 212)**	**now (p. 214)**
date (p. 203)	**key (p. 213)**	**send-lifetime (p. 216)**
duration (p. 210)	**key-string (p. 214)**	**time (p. 218)**

accept-lifetime

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime

  ```
  Set key accept lifetime.
  ```

  Next Available Options:
  - **date** -- Key accept start date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **now** -- Use current day and time.**(p. 214)**
  - **infinite** -- Set infinite lifetime.**(p. 212)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime

  ```
  Set key accept lifetime.
  ```

  Next Available Options:
  - **date** -- Key accept start date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **now** -- Use current day and time.**(p. 214)**
  - **infinite** -- Set infinite lifetime.**(p. 212)**

date

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE]*

  ```
  Key accept start date.
  ```

  Next Available Option:
  - **time** -- Key accept start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE]*

  ```
  Key accept stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

© 2007 Hewlett-Packard Development Company, L.P.

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE]*

  `Key send start date.`

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE]*

  `Key send stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now *[DATE]*

  `Key send stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE]*

  `Key send start date.`

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE]*

  `Key send stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now *[DATE]*

  `Key send stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE]*

  `Key accept stop date.`

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE]*

```
Key send start date.
```

Next Available Option:
- **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime now *[DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]*

```
Key send start date.
```

Next Available Option:
- **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime now *[DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

© 2007 Hewlett-Packard Development Company, L.P.

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE] [TIME] [DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE]*

  ```
  Key send start date.
  ```

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE] [TIME] [DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime now *[DATE]*

  ```
  Key send stop date.
  ```

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE]*

  ```
  Key accept start date.
  ```

  Next Available Option:
  - **time** -- Key accept start time. (HH:MM[:SS]) **(p. 218)**

© 2007 Hewlett-Packard Development Company, L.P.

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE]*

  `Key accept stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE]*

  `Key send start date.`

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE]*

  `Key send stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now *[DATE]*

  `Key send stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE]*

  `Key send start date.`

  Next Available Option:
  - **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE]*

  `Key send stop date.`

  Next Available Option:
  - **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now *[DATE]*

  `Key send stop date.`

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE]*

```
Key accept stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE]*

```
Key send start date.
```

Next Available Option:
- **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime now *[DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE]*

```
Key send start date.
```

Next Available Option:
- **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime now *[DATE]*

© 2007 Hewlett-Packard Development Company, L.P.

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE]*

```
Key send start date.
```

Next Available Option:
- **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE] [TIME] [DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime now *[DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE]*

```
Key send start date.
```

Next Available Option:
- **time** -- Key send start time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE] [TIME] [DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime now *[DATE]*

```
Key send stop date.
```

Next Available Option:
- **time** -- Key send stop time. (HH:MM[:SS]) **(p. 218)**

© 2007 Hewlett-Packard Development Company, L.P.

duration

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER*

  `Use current day and time.`

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 216)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime now duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER*

  `Use current day and time.`

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 216)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime now duration *NUMBER*

  `Use current day and time.`

© 2007 Hewlett-Packard Development Company, L.P.

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE] [TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 216)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER*

  ```
  Use current day and time.
  ```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **send-lifetime** -- Set key send lifetime.**(p. 216)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime now duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE] [TIME]* duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime now duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE] [TIME]* duration *NUMBER*

  `Use current day and time.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime now duration *NUMBER*

  `Use current day and time.`

infinite

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite

  `Set infinite lifetime.`

Next Available Option:
- **send-lifetime** -- Set key send lifetime.**(p. 216)**

© 2007 Hewlett-Packard Development Company, L.P.

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite

  `Set infinite lifetime.`

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 216)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime infinite

  `Set infinite lifetime.`

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime infinite

  `Set infinite lifetime.`

key

- [no] key-chain *KEY-CHAIN* key *< 0 to 255 >*

  `Configure chain keys.`

  Range: < 0 to 255 >

  Next Available Options:
  - **key-string** -- Set key string (ASCII-STR) **(p. 214)**
  - **accept-lifetime** -- Set key accept lifetime.**(p. 203)**
  - **send-lifetime** -- Set key send lifetime.**(p. 216)**

© 2007 Hewlett-Packard Development Company, L.P.

key-string

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING*

```
Set key string
```

Next Available Options:
- **accept-lifetime** -- Set key accept lifetime.**(p. 203)**
- **send-lifetime** -- Set key send lifetime.**(p. 216)**

now

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime now

```
Use current day and time.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**

© 2007 Hewlett-Packard Development Company, L.P.

- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime now

```
Use current day and time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

send-lifetime

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime

```
Set key send lifetime.
```

Next Available Options:
- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
- **now** -- Use current day and time.**(p. 214)**
- **infinite** -- Set infinite lifetime.**(p. 212)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime

```
Set key send lifetime.
```

Next Available Options:
- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
- **now** -- Use current day and time.**(p. 214)**
- **infinite** -- Set infinite lifetime.**(p. 212)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime

```
Set key send lifetime.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:
- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
- **now** -- Use current day and time.**(p. 214)**
- **infinite** -- Set infinite lifetime.**(p. 212)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime

```
Set key send lifetime.
```

Next Available Options:
- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
- **now** -- Use current day and time.**(p. 214)**
- **infinite** -- Set infinite lifetime.**(p. 212)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime

```
Set key send lifetime.
```

Next Available Options:
- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
- **now** -- Use current day and time.**(p. 214)**
- **infinite** -- Set infinite lifetime.**(p. 212)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime

```
Set key send lifetime.
```

Next Available Options:
- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
- **now** -- Use current day and time.**(p. 214)**
- **infinite** -- Set infinite lifetime.**(p. 212)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime

```
Set key send lifetime.
```

Next Available Options:
- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
- **now** -- Use current day and time.**(p. 214)**
- **infinite** -- Set infinite lifetime.**(p. 212)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime

```
Set key send lifetime.
```

Next Available Options:
- **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
- **now** -- Use current day and time.**(p. 214)**
- **infinite** -- Set infinite lifetime.**(p. 212)**

© 2007 Hewlett-Packard Development Company, L.P.

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime

  `Set key send lifetime.`

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **now** -- Use current day and time.**(p. 214)**
  - **infinite** -- Set infinite lifetime.**(p. 212)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime

  `Set key send lifetime.`

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **now** -- Use current day and time.**(p. 214)**
  - **infinite** -- Set infinite lifetime.**(p. 212)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime

  `Set key send lifetime.`

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **now** -- Use current day and time.**(p. 214)**
  - **infinite** -- Set infinite lifetime.**(p. 212)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime

  `Set key send lifetime.`

  Next Available Options:
  - **date** -- Key send start date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **now** -- Use current day and time.**(p. 214)**
  - **infinite** -- Set infinite lifetime.**(p. 212)**

time

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]*

  `Key accept start time.`

  Next Available Options:
  - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]*

  `Key send stop time.`

  Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **send-lifetime** -- Set key send lifetime.**(p. 216)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME]*

```
Key send start time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

```
Key send stop time.
```

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now *[DATE] [TIME]*

```
Key send stop time.
```

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME]*

```
Key send start time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

```
Key send stop time.
```

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now *[DATE] [TIME]*

```
Key send stop time.
```

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]*

```
Key send stop time.
```

Next Available Option:
- **send-lifetime** -- Set key send lifetime.**(p. 216)**

■ key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME]*

```
Key send start time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**

© 2007 Hewlett-Packard Development Company, L.P.

- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now *[DATE] [TIME]* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime now duration *NUMBER* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* accept-lifetime infinite send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**

© 2007 Hewlett-Packard Development Company, L.P.

- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* key-string *KEY-STRING* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]*

  ```
  Key accept start time.
  ```

  Next Available Options:
  - **date** -- Key accept stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 216)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME] [DATE] [TIME]* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

© 2007 Hewlett-Packard Development Company, L.P.

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime *[DATE] [TIME]* duration *NUMBER* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

  Next Available Option:
  - **send-lifetime** -- Set key send lifetime.**(p. 216)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now *[DATE] [TIME]* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME]*

  ```
  Key send start time.
  ```

  Next Available Options:
  - **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
  - **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime now duration *NUMBER* send-lifetime now *[DATE] [TIME]*

  ```
  Key send stop time.
  ```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE] [TIME]*

© 2007 Hewlett-Packard Development Company, L.P.

```
Key send start time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime *[DATE] [TIME] [DATE] [TIME]*

```
Key send stop time.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* accept-lifetime infinite send-lifetime now *[DATE] [TIME]*

```
Key send stop time.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE] [TIME]*

```
Key send start time.
```

Next Available Options:
- **date** -- Key send stop date. (MM/DD[/[YY]YY]) **(p. 203)**
- **duration** -- Use current day and time. (NUMBER) **(p. 210)**

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime *[DATE] [TIME] [DATE] [TIME]*

```
Key send stop time.
```

- key-chain *KEY-CHAIN* key *< 0 to 255 >* send-lifetime now *[DATE] [TIME]*

```
Key send stop time.
```

© 2007 Hewlett-Packard Development Company, L.P.

kill

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show ssh (page 382)** **show telnet (page 385)**

```
Usage: kill [SESSION_ID]

Description: Kill other active console, telnet, or ssh sessions. The session from
             which you enter the command is not terminated.
             If no session ID is specified, all other active sessions
             are terminated.
```

NOTES

About Termination

The command does not terminate a Console session on the serial port, either on a direct connection or through a terminal server or modem.

COMMAND STRUCTURE

- kill **session < (Range unavailble) >** -- Kill other active console, telnet, or ssh sessions **(p. 225)**

EXAMPLES

Example: kill SESSION-ID

Display the currently active management sessions, then terminate one of the Telnet sessions:

```
ProCurve# show telnet

 Telnet Activity

  Session Privilege From            To
  ------- --------- --------------- ---------------
        1 Superuser Console
    **  2 Manager    10.132.193.146
        3 Manager    10.132.193.101

ProCurve# kill 3
ProCurve# show telnet

 Telnet Activity

  Session Privilege From            To
  ------- --------- --------------- ---------------
        1 Superuser Console
    **  2 Manager    10.132.193.146
```

© 2007 Hewlett-Packard Development Company, L.P.

COMMAND DETAILS

session (p. 225)

session

- kill *< (1-6) >*

```
Usage: kill [SESSION_ID]

Description: Kill other active console, telnet, or ssh sessions.
             If no session ID is specified, all other active sessions
             are terminated.
```

Range: < (1-6) >

© 2007 Hewlett-Packard Development Company, L.P.

licenses

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: licenses <hardware-id PKG-ID |
                 install PKG-ID PKG-KEY |
                 uninstall PKG-ID>

Description: Manage premium features.

Parameters:

    o hardware-id - Display the hardware ID for installing the specified
                    package on this chassis.
    o install     - Install the specified package.
    o uninstall   - Uninstall the specified package, and display the
                    uninstall verification key.
```

COMMAND STRUCTURE

- licenses **hardware-id < premium-edge >** -- Display hardware ID for installation request. **(p. 226)**
- licenses **install < premium-edge >** -- Install the specified package. **(p. 226)**
  - **key** -- Enter key for this feature. (ASCII-STR) **(p. 227)**
- licenses **uninstall < premium-edge >** -- Uninstall the specified package. **(p. 227)**

COMMAND DETAILS

hardware-id (p. 226)	**key (p. 227)**
install (p. 226)	**uninstall (p. 227)**

hardware-id

- licenses hardware-id *< premium-edge >*

```
Display hardware ID for installation request.
```

Supported Values:
- **premium-edge**

install

- licenses install *< premium-edge >*

```
Install the specified package.
```

Supported Values:
- **premium-edge**

Next Available Option:
- **key** -- Enter key for this feature. (ASCII-STR) **(p. 227)**

© 2007 Hewlett-Packard Development Company, L.P.

key

- licenses install *< premium-edge > KEY*

```
Enter key for this feature.
```

uninstall

- licenses uninstall *< premium-edge >*

```
Uninstall the specified package.
```

Supported Values:

- **premium-edge**

© 2007 Hewlett-Packard Development Company, L.P.

link-keepalive

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: link-keepalive interval <10-100>
       link-keepalive retries <3-10>

Description: Configure UDLD on your switch.
             The first version of the command is used to configure
             keep-alive interval in seconds. Here 10 is 1 sec, 11 is 1.1 sec,
             and so on. Default keep-alive interval is 5 seconds.
             The second version of the command is used to configure
             maximum number of keep-alive attempts. Default keep-alive
             attempt is 4.
```

COMMAND STRUCTURE

- link-keepalive **interval < 10 to 100 >** -- Set link keep-alive interval in deciseconds. **(p. 228)**
- link-keepalive **retries < 3 to 10 >** -- Set maximum number of link keep-alive attempts. **(p. 228)**

COMMAND DETAILS

interval (p. 228) **retries (p. 228)**

interval

- link-keepalive interval *< 10 to 100 >*

```
Set link keep-alive interval in deciseconds.
```

Range: < 10 to 100 >

retries

- link-keepalive retries *< 3 to 10 >*

```
Set maximum number of link keep-alive attempts.
```

Range: < 3 to 10 >

© 2007 Hewlett-Packard Development Company, L.P.

link-test

OVERVIEW

Category:	
Primary context:	operator
Related Commands	ping (page 263)

```
Usage: link-test MAC-ADDR [vlan <VLAN-ID>] [repetitions <1-999>]
                          [timeout <1-256>]

Description: Test the connection to a MAC address on the LAN.
             The command sends a 802.2 test packet to a specific target
             node on a network directly attached to a port in that
             LAN. The target node must be able to respond to this test
             packet with an 802.2 Test Response packet in order for the
             test to work. The switch produces the following output if
             the link test succeeds: 'Link-test passed'; otherwise, the
             following is displayed: 'Link-test timed out'.

Parameters:

    o MAC-ADDR  - MAC address of the station to which to send link test.

    o [vlan VLAN-ID] - Expected VLAN on which the station is expected to
      be present. If this argument is not present then the VLAN used is 1.

    o [repetitions <1-999>] - Number of test packets to send; the
      default value is 1.

    o [timeout <1-256>] - Seconds within which a response is required
      before the test is considered as failed; the default value is 5.

Examples:

    (1) hp-switch#  link-test 0800095F3AD6
```

COMMAND STRUCTURE

- link-test **mac** -- MAC address of the station to which to send link test. (MAC-ADDR) (p. 230)
- link-test **repetitions < 1 to 999 >** -- Number of test packets to send <1-999>. (NUMBER) (p. 230)
- link-test **timeout < 0 to 256 >** -- Test timeout in seconds <0-256>. (NUMBER) (p. 230)
- link-test **vlan** -- VLAN on which the tested station is to be present. (VLAN-ID) (p. 230)

EXAMPLES

Example: link-test

Test the link to MAC address 0800095F3AD6 on VLAN 1:

```
ProCurve# link-test 0800095F3AD6
```

© 2007 Hewlett-Packard Development Company, L.P.

COMMAND DETAILS

mac (p. 230)	timeout (p. 230)
repetitions (p. 230)	vlan (p. 230)

mac

- link-test *MAC-ADDR*

```
MAC address of the station to which to send link test.
```

repetitions

- link-test repetitions *< 1 to 999 >*

```
Number of test packets to send <1-999>.
```

Range: < 1 to 999 >

timeout

- link-test timeout *< 0 to 256 >*

```
Test timeout in seconds <0-256>.
```

Range: < 0 to 256 >

vlan

- link-test vlan *VLAN-ID*

```
VLAN on which the tested station is to be present.
```

© 2007 Hewlett-Packard Development Company, L.P.

lldp

OVERVIEW

Category:	Device Discovery
Primary context:	config
Related Commands	**show lldp (page 362)**

```
Usage:lldp ...

Description: Configuration for LLDP parameter. Provides a standards-based method
             for enabling the switches to advertise themselves to adjacent devices
             and to learn about adjacent LLDP devices.
             You can also configure the Media Extension Discovery (MED) extension
             to LLDP for Voice over IP (VoIP) devices.
```

COMMAND STRUCTURE

- lldp **admin-status** -- Set the port in one of the operational mode transmit | receive | transmit & receive | disable the port ([ethernet] PORT-LIST) **(p. 232)**
  - **omodes < TxOnly | RxOnly | Tx_Rx | ... >** -- Set the operational mode: transmit | receive | transmit-receive | disable. (NUMBER) **(p. 236)**
- [no] lldp **config** -- Specify configurational parameters to the port ([ethernet] PORT-LIST) **(p. 234)**
  - **basicTlvEnable < port_descr | system_name | system_descr | ... >** -- Specify the Basic TLV List to be advertised. (NUMBER) **(p. 233)**
  - **dot3TlvEnable < macphy_config >** -- Specify the 802.3 TLV List to be advertised. (NUMBER) **(p. 234)**
  - **ipAddrEnable** -- Set IP ADDR to be enabled. (IP-ADDR) **(p. 235)**
  - **medPortLocation** -- Configure location-id information to be advertised. **(p. 235)**
    - **civic-addr** -- Specify the civic location-id information to be advertised **(p. 233)**
      - **COUNTRY** -- Specify the Country Code of two characters. (ASCII-STR) **(p. 234)**
        - **WHAT** -- Specify the 'what' number of range <0-2>. (NUMBER) **(p. 236)**
          - **CA-TYPE** -- Specify the ca-type value of range <0-255>. (NUMBER) **(p. 233)**
            - **CA-VALUE** -- Specify the ca-value string. (ASCII-STR) **(p. 233)**
    - **elin-addr** -- Specify the elin address location to be advertised. **(p. 235)**
      - **addr** -- Specify the Location name to be advertised. (OCTET-STR) **(p. 232)**
  - **medTlvEnable < capabilities | network_policy | location_id | ... >** -- Specify the MED TLV List to be advertised. (NUMBER) **(p. 236)**
- [no] lldp **enable-notification** -- Set the port for which notification should be enabled ([ethernet] PORT-LIST) **(p. 235)**
- lldp **fast-start-count < 1 to 10 >** -- Set MED fast-start count in seconds (NUMBER) **(p. 235)**
- lldp **holdtime-multiplier < 2 to 10 >** -- Set holdtime-multipler between <2-10>; the default is 4 (NUMBER) **(p. 235)**
- lldp **refresh-interval < 5 to 32768 >** -- Set refresh interval/transmit-interval in seconds (NUMBER) **(p. 236)**
- [no] lldp **run** -- Start or Stop LLDP on device **(p. 236)**
- [no] lldp **top-change-notify** -- Set the port for which LLDP MED topology notification should be enabled ([ethernet] PORT-LIST) **(p. 236)**

© 2007 Hewlett-Packard Development Company, L.P.

EXAMPLES

Example: lldp config basicTlvEnable

Exclude the system name from the outbound LLDP advertisements for all ports:

```
ProCurve(config)# no lldp config A1-A24 basicTlvEnable system_name
```

Example: lldp config ipAddrEnable

Use a secondary IP address in LLDP advertisements. In this example, use secondary IP address 10.10.10.100, which is on a subnetted VLAN that contains port 3:

```
ProCurve(config)# lldp config 3 ipAddrEnable 10.10.10.100
```

Example: lldp enable-notification

Enable SNMP notification on ports 1 - 5:

```
ProCurve(config)# lldp enable-notification A1-A5
```

Example: lldp holdtime-multiplier

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 * 15). To reduce the Time-to-Live, lower the holdtime-interval to 2, which results in a Time-to-Live of 30 seconds:

```
ProCurve(config)# lldp holdtime-multiplier 2
```

Example: lldp run

Disable LLDP on the switch:

```
ProCurve(config)# no lldp run
```

COMMAND DETAILS

addr (p. 232)	COUNTRY (p. 234)	medPortLocation (p. 235)
admin-status (p. 232)	dot3TlvEnable (p. 234)	medTlvEnable (p. 236)
basicTlvEnable (p. 233)	elin-addr (p. 235)	omodes (p. 236)
CA-TYPE (p. 233)	enable-notification (p. 235)	refresh-interval (p. 236)
CA-VALUE (p. 233)	fast-start-count (p. 235)	run (p. 236)
civic-addr (p. 233)	holdtime-multiplier (p. 235)	top-change-notify (p. 236)
config (p. 234)	ipAddrEnable (p. 235)	WHAT (p. 236)

addr

- lldp config *[ETHERNET] PORT-LIST* medPortLocation elin-addr *OCTET-STR*

```
Specify the Location name to be advertised.
```

admin-status

- lldp admin-status *[ETHERNET] PORT-LIST*

```
Usage: lldp admin-status <port-list> <txonly | rxonly
                                      tx_rx | disable>

Description: Set the port in one of the operational mode
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                transmit | receive | transmit & receive |
                disable the port.
```

Next Available Option:

- **omodes** < TxOnly | RxOnly | Tx_Rx | ... > -- Set the operational mode: transmit | receive | transmit-receive | disable. (NUMBER) **(p. 236)**

basicTlvEnable

- [no] lldp config *[ETHERNET] PORT-LIST* basicTlvEnable *< port_descr | system_name | system_descr | ... >*

```
Specify the Basic TLV List to be advertised.
```

Supported Values:

- **port_descr** -- Port Description TLV
- **system_name** -- System Name TLV
- **system_descr** -- System Description TLV
- **system_cap** -- System Capability TLV

CA-TYPE

- lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr *COUNTRY NUMBER NUMBER*

```
Specify the ca-type value of range <0-255>.
```

Next Available Option:

- **CA-VALUE** -- Specify the ca-value string. (ASCII-STR) **(p. 233)**

CA-VALUE

- lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr *COUNTRY NUMBER NUMBER CA-VALUE*

```
Specify the ca-value string.
```

civic-addr

- [no] lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr

```
Usage: lldp config <port-list> medPortLocation civic-str <COUNTRY-STR>
                                  <WHAT> <CA-TYPE> <CA-VALUE>

Description: Specify the civic location-id information to be advertised.
             The total length of the TLV is 104.
             COUNTRY-STR : Set the Country Code of two characters.e.g. DE or US.
             WHAT        : Set the 'what' number of range <0-2>.
                           0 - Location of DHCP server.
                           1 - Location of Switch.
                           2 - Location of Client.
             CA-TYPE     : Set the ca-type of range <0-255>.
                           It is a repeatable parameter.ca-type should be unique.
                           ca-type sholud be followed by ca-value.
             CA-VALUE    : Set the ca-value string.
```

Next Available Option:

- **COUNTRY** -- Specify the Country Code of two characters. (ASCII-STR) **(p. 234)**

© 2007 Hewlett-Packard Development Company, L.P.

config

- lldp config *[ETHERNET] PORT-LIST*

```
Usage: [no] lldp config <PORT-LIST> <basicTlvEnable TLVMAP |
                                    dot3TlvEnable  TLVMAP |
                                    ipAddrEnable IP-ADDR  |
                                    medPortLocation ...   |
                                    medTlvEnable   TLVMAP>

Description: Specify configurational parameters to the port.
             Set basicTlvEnable with any one of the following TLV Maps.
                 port_descr     : Send Port Description TLV out this port.
                 system_name    : Send System Name TLV out this port.
                 system_descr   : Send System Descr TLV out this port.
                 system_cap     : Send Capability TLV out this port.
             Set dot3TlvEnable with the following TLV Map.
                 macphy_config  : Send Mac Phy Config TLV out this port.
             Set ipAddrEnable with the IP-ADDR to send out this port.
             Set medPortLocation with location information for the port.
                 civic-addr     : Set civic address to send out this port.
                 elin-addr      : Set elin address to send out this port.
             Set medTlvEnable with any one of the following TLV Maps.
                 capabilities   : Send Capability TLV out this port.This TLV has
                                  to be enabled first to enable any MED TLV's.
                 network_policy : Send Network Policy TLV out this port.
                 location_id    : Send Location Id TLV out this port.
                 poe            : Send Med Poe TLV out this port.
```

Next Available Options:

- **basicTlvEnable** < port_descr | system_name | system_descr | ... > -- Specify the Basic TLV List to be advertised. (NUMBER) **(p. 233)**
- **ipAddrEnable** -- Set IP ADDR to be enabled. (IP-ADDR) **(p. 235)**
- **medTlvEnable** < capabilities | network_policy | location_id | ... > -- Specify the MED TLV List to be advertised. (NUMBER) **(p. 236)**
- **medPortLocation** -- Configure location-id information to be advertised. **(p. 235)**
- **dot3TlvEnable** < macphy_config > -- Specify the 802.3 TLV List to be advertised. (NUMBER) **(p. 234)**

COUNTRY

- lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr *COUNTRY*

```
Specify the Country Code of two characters.
```

Next Available Option:

- **WHAT** -- Specify the 'what' number of range <0-2>. (NUMBER) **(p. 236)**

dot3TlvEnable

- [no] lldp config *[ETHERNET] PORT-LIST* dot3TlvEnable *< macphy_config >*

```
Specify the 802.3 TLV List to be advertised.
```

Supported Values:

© 2007 Hewlett-Packard Development Company, L.P.

- **macphy_config** -- MAC Physical Config Tlv

elin-addr

- [no] lldp config *[ETHERNET] PORT-LIST* medPortLocation elin-addr

```
Specify the elin address location to be advertised.
```

Next Available Option:

- **addr** -- Specify the Location name to be advertised. (OCTET-STR) **(p. 232)**

enable-notification

- [no] lldp enable-notification *[ETHERNET] PORT-LIST*

```
Usage: [no] lldp notificationEnable <PORT-LIST>

Description: Set the port for which notification should be enabled.
```

fast-start-count

- lldp fast-start-count *< 1 to 10 >*

```
Usage: lldp fast-start-count <1-10>

Description: Set MED fast-start count in seconds.
```

Range: < 1 to 10 >

holdtime-multiplier

- lldp holdtime-multiplier *< 2 to 10 >*

```
Usage: lldp holdtime-multiplier <2-10>

Description: Set holdtime-multipler between <2-10>; the default is 4.
```

Range: < 2 to 10 >

ipAddrEnable

- [no] lldp config *[ETHERNET] PORT-LIST* ipAddrEnable *IP-ADDR*

```
Set IP ADDR to be enabled.
```

medPortLocation

- [no] lldp config *[ETHERNET] PORT-LIST* medPortLocation

```
Configure location-id information to be advertised.
```

Next Available Options:

- **civic-addr** -- Specify the civic location-id information to be advertised**(p. 233)**
- **elin-addr** -- Specify the elin address location to be advertised. **(p. 235)**

© 2007 Hewlett-Packard Development Company, L.P.

medTlvEnable

- [no] lldp config *[ETHERNET] PORT-LIST* medTlvEnable *< capabilities | network_policy | location_id | ... >*

```
Specify the MED TLV List to be advertised.
```

Supported Values:
- **capabilities** -- Capability TLV
- **network_policy** -- Network Policy TLV
- **location_id** -- Location Id TLV
- **poe** -- Poe TLV

omodes

- lldp admin-status *[ETHERNET] PORT-LIST < TxOnly | RxOnly | Tx_Rx | ... >*

```
Set the operational mode: transmit | receive |
transmit-receive | disable.
```

Supported Values:
- **TxOnly** -- Set in transmit mode.
- **RxOnly** -- Set in receive mode.
- **Tx_Rx** -- Set in transmit & Receive mode.
- **disable** -- disable.

refresh-interval

- lldp refresh-interval *< 5 to 32768 >*

```
Usage: lldp refresh-interval <5-32768>

Description: Set refresh interval/transmit-interval in seconds.
             The default is 30.
             The refresh interval/transmit-interval should be greater
             than or equal to (4*delay-interval).
             The default value of delay-interval is 2.
```

Range: < 5 to 32768 >

run

- [no] lldp run

```
Usage:[no] lldp run

Description: Start or Stop LLDP on device.
```

top-change-notify

- [no] lldp top-change-notify *[ETHERNET] PORT-LIST*

```
Usage:[no] lldp top-change-notify <port-list>

Description: Set the port for which LLDP MED topology notification should be enabled.
```

WHAT

- lldp config *[ETHERNET] PORT-LIST* medPortLocation civic-addr *COUNTRY NUMBER*

```
Specify the 'what' number of range <0-2>.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:

- **CA-TYPE** -- Specify the ca-type value of range <0-255>. (NUMBER) **(p. 233)**

© 2007 Hewlett-Packard Development Company, L.P.

lockout-mac

OVERVIEW

Category:	Port Security
Primary context:	config
Related Commands	**show lockout-mac (page 363)**

```
Usage: lockout-mac <MAC-ADDR>

Description: Lock out a MAC address. The switch drops all traffic to or from
             the locked out address.

Parameter:

    o MAC-ADDR  - MAC address to lock down.

Examples:

    (1) ProCurve(config)#  lockout-mac 0800095F3AD6
```

NOTES

Per Switch Lockout

MAC Lockout is implemented on a per switch assignment.

EXAMPLES

Example: lockout-mac

Drop all traffic to or from MAC address 0800095F3AD6:

```
ProCurve# lockout-mac 0800095F3AD6
```

© 2007 Hewlett-Packard Development Company, L.P.

log

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	logging (page 241) show logging (page 363)

```
Usage: log [-a|-r|-m|-p|-w|-i|-d|substring ...]

Description: Display log events.
             -a - Instructs the switch to display all recorded log
             events, which includes events from previous boot cycles.
             -r - Instructs the switch to display recorded
             log events in reverse order (most recent first).
             substring - Instructs the switch to display
             only those events that match the substring.

             The remaining event class options (listed below in
             order of severity - lowest severity first) confine
             output to event clases of equal or higher severity
             -d - Debug
             -i - Informative
             -w - Warnings
             -p - Performance
             -m - Major
             Only one of options -d,-i,-w,-p and -m may be specified.

             The -a, -r, and substring options may be used in
             combination with an event class option.
```

COMMAND STRUCTURE

- log **-a** -- Display all log events, including those from previous boot cycles. (p. 239)
- log **event_class < -M | -P | -W | ... >** -- Specify substring to match in log entry. See 'log help' for details. (p. 239)
- log **option** -- Specify substring to match in log entry. See 'log help' for details. (ASCII-STR) (p. 240)
- log **-r** -- Display log events in reverse order (most recent first). (p. 240)

COMMAND DETAILS

-a (p. 239)	option (p. 240)
event_class (p. 239)	-r (p. 240)

-a

- log -a

```
Display all log events, including those from previous boot cycles.
```

event_class

- log

```
Specify substring to match in log entry. See 'log help' for details.
```

© 2007 Hewlett-Packard Development Company, L.P.

Supported Values:

- **-M** -- Major event class.
- **-P** -- Performance event class.
- **-W** -- Warning event class.
- **-I** -- Information event class.
- **-D** -- Debug event class.

option

- log *OPTION*

```
Specify substring to match in log entry. See 'log help' for details.
```

-r

- log -r

```
Display log events in reverse order (most recent first).
```

© 2007 Hewlett-Packard Development Company, L.P.

logging

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	log (page 239) show logging (page 363)

```
Usage: [no] logging <IP_ADDR>
       [no] logging facility <facility>

Description: Add an IP address to the list of receiving syslog servers.
             Use of 'no' without an IP address specified will remove all
             IP addresses from the list of syslog receivers. If an IP
             address is specified, that receiver will be removed.
             Specify syslog server facility with <facility>. Use of
             'no' sets the facility back to defaults.
```

COMMAND STRUCTURE

- [no] logging **facility < kern | user | mail | ... >** -- Specify the syslog facility value that will be used for all syslog servers (p. 241)
- [no] logging **ip-address** -- Add an IP address to the list of receiving syslog servers (IP-ADDR) (p. 242)

COMMAND DETAILS

facility (p. 241)	ip-address (p. 242)

facility

- [no] logging facility *< kern | user | mail | ... >*

```
Description: Specify the syslog facility value that will be used
             for all syslog servers. Syslog facility determines
             where syslog servers should log the syslog message.
```

Supported Values:

- **kern**
- **user**
- **mail**
- **daemon**
- **auth**
- **syslog**
- **lpr**
- **news**
- **uucp**
- **sys9**
- **sys10**
- **sys11**
- **sys12**
- **sys13**
- **sys14**

© 2007 Hewlett-Packard Development Company, L.P.

- **cron**
- **local0**
- **local1**
- **local2**
- **local3**
- **local4**
- **local5**
- **local6**
- **local7**

ip-address

- [no] logging *IP-ADDR*

```
Usage: [no] logging <IP_ADDR>
       [no] logging facility <facility>

Description: Add an IP address to the list of receiving syslog servers.
             Use of 'no' without an IP address specified will remove all
             IP addresses from the list of syslog receivers. If an IP
             address is specified, that receiver will be removed.
             Specify syslog server facility with <facility>. Use of
             'no' sets the facility back to defaults.
```

© 2007 Hewlett-Packard Development Company, L.P.

log-numbers

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] log-numbers

Description: Enable the display of log event numbers when log is displayed
             via the CLI or via the menu.
```

© 2007 Hewlett-Packard Development Company, L.P.

logout

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	

```
Usage: logout

Description: Terminate this console/telnet session.
```

© 2007 Hewlett-Packard Development Company, L.P.

loop-protect

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] loop-protect <...>
            [[ethernet] PORT-LIST [receiver-action <send-disable|no-disable>]|
            [transmit-interval <1-10>]|
            [disable-period <0-604800>]|
            [trap <loop-detected>]

Description: Configure Loop protection on the switch.


Parameters:
 o ethernet PORT-LIST - Port(s) to configure loop protection on. By default
                        loop protection is disabled on a port
 o receiver-action    - Sets the loop detected action per port. When a loop
                        is detected the port that received the loop protection
                        packet determines the action taken. If send-disable
                        is selected the port that transmitted the packet will
                        be disabled. If no-disable is selected, the port will
                        not be disabled. The default action is 'send-disable'.
 o trap <loop-detected> - Configure Loop protection traps. The following
                          traps are generated by Loop protection
                        - 'loop-detected' signifies that a loop was detected
                           on a port.
 o disable-timer <0-604800> (default:0) - Sets the time in seconds to
                        disable a port for when a loop has been detected. A
                        value of 0 disables the auto reenable functionality.
                        By default the timer is disabled.

 o transmit-interval <1-10> (default:5) - Time in seconds between transmission
                                          of loop protection packets.
```

COMMAND STRUCTURE

- loop-protect **disable-timer < 0 to 604800 >** -- Set time in seconds to wait before attempting to reenable a port. (NUMBER) **(p. 246)**
- [no] loop-protect **port-list** -- Specify the ports that are to be added to/removed from loop protection. ([ethernet] PORT-LIST) **(p. 246)**
  - **receiver-action < send-disable | no-disable >** -- Select action to take when loop protect packets are received on the specified port(s). **(p. 246)**
- loop-protect **transmit-interval < 1 to 10 >** -- Set time between packet transmissions. (NUMBER) **(p. 246)**
- [no] loop-protect **trap** -- Specify loop protection traps that are to be enabled/disabled. **(p. 246)**
  - **loop-detected** -- generate trap when a loop is detected **(p. 246)**

COMMAND DETAILS

disable-timer (p. 246)	**port-list (p. 246)**	**transmit-interval (p. 246)**
loop-detected (p. 246)	**receiver-action (p. 246)**	**trap (p. 246)**

© 2007 Hewlett-Packard Development Company, L.P.

disable-timer

- loop-protect disable-timer *< 0 to 604800 >*

  `Set time in seconds to wait before attempting to reenable a port.`

  Range: < 0 to 604800 >

loop-detected

- [no] loop-protect trap loop-detected

  `generate trap when a loop is detected`

port-list

- [no] loop-protect *[ETHERNET] PORT-LIST*

  `Specify the ports that are to be added to/removed from loop protection.`

  Next Available Option:
  - **receiver-action** < send-disable | no-disable > -- Select action to take when loop protect packets are received on the specified port(s). **(p. 246)**

receiver-action

- loop-protect *[ETHERNET] PORT-LIST* receiver-action *< send-disable | no-disable >*

  `Select action to take when loop protect packets are received on the specified port(s).`

  Supported Values:
  - **send-disable**
  - **no-disable**

transmit-interval

- loop-protect transmit-interval *< 1 to 10 >*

  `Set time between packet transmissions.`

  Range: < 1 to 10 >

trap

- [no] loop-protect trap

  `Specify loop protection traps that are to be enabled/disabled.`

  Next Available Option:
  - **loop-detected** -- generate trap when a loop is detected**(p. 246)**

© 2007 Hewlett-Packard Development Company, L.P.

mac-age-time

OVERVIEW

Category:	Device Discovery
Primary context:	config
Related Commands	

```
Usage: mac-age-time <60-999960>

Description: Set the MAC address table's age-out interval.
             A MAC address that is dynamically learned by the switch, stays
             in the switch's address table for a certain amount of time -
             the age-out interval, before being aged out. An address is aged
             out if the switch does not receive traffic from that MAC
             address for the age-out interval. The interval is measured in
             seconds. The default value is 300 seconds.
```

EXAMPLES

Example: mac-age-time SECONDS

Configure the MAC age-out interval to seven minutes:

```
ProCurve(config)# mac-age-time 420
```

© 2007 Hewlett-Packard Development Company, L.P.

management-vlan

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**show vlan (page 390)**

```
Usage: [no] management-vlan VLAN-ID

Description: Set the VLAN that is to be used as the management VLAN.
```

EXAMPLES

Example: management-vlan

Set VLAN 100 as the management VLAN and add ports A1 and A2 to it:

```
ProCurve(config)# management-vlan 100
ProCurve(config)# vlan 100 tagged a1
ProCurve(config)# vlan 100 tagged a2
```

© 2007 Hewlett-Packard Development Company, L.P.

max-vlans

OVERVIEW

Category:	VLANs
Primary context:	config
Related Commands	

```
Usage: max-vlans <1-2048>

Description: Set the maximum number of VLANs on the switch.
             The default is 256.
```

EXAMPLES

Example: max-vlans NUMBER

Reconfigure the switch to allow 10 VLANs:

```
HPswitch(config)# max-vlans 10
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

© 2007 Hewlett-Packard Development Company, L.P.

menu

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	

```
Usage: menu

Description: Change console user interface to menu system.
```

EXAMPLES

menu

Enter the menu mode for switch configuration:

```
ProCurve# menu

HP ProCurve Switch 5400zl                              1-Jan-2006   4:55:06
=======================- TELNET - MANAGER MODE -=========================
                                  Main Menu

   1. Status and Counters...
   2. Switch Configuration...
   3. Console Passwords...
   4. Event Log
   5. Command Line (CLI)
   6. Reboot Switch
   7. Download OS
   8. Run Setup
   0. Logout


Provides the menu to display configuration, status, and counters.
To select menu item, press item number, or highlight item and press <Enter>.
```

© 2007 Hewlett-Packard Development Company, L.P.

mesh

OVERVIEW

Category:	Redundant Paths
Primary context:	config
Related Commands	**show mesh (page 365)**

```
Usage: [no] mesh [ethernet] PORT-LIST

Description: Configure the specified ports as being members of a mesh group.
             A mesh group can have up to 24 member ports.

           - VLAN support must be enabled before configuring a mesh group.
           - A mesh group cannot exist if IP routing is enabled.  Disable
             routing protocols (if any) before configuring a mesh group.
           - After configuring meshing, it will be necessary to reboot the
             switch before the changes take effect.
```

COMMAND STRUCTURE

- [no] mesh **portlist** -- Specify the ports that are to be added to/removed from a mesh. ([ethernet] PORT-LIST) **(p. 251)**

EXAMPLES

Example: mesh PORT-LIST

Configure meshing on ports A1-A4, B3, C1, and D1-D3:

```
HPswitch(config)# mesh e a1-a4,b3,c1,d1-d3
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

COMMAND DETAILS

portlist (p. 251)

portlist

- [no] mesh *[ETHERNET] PORT-LIST*

```
Specify the ports that are to be added to/removed from a mesh.
```

mirror

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: 1) mirror <1-4> [ name NAME-STR ] port PORT-NUM
       2) mirror <1-4> [ name NAME-STR ] remote ip SRC-IP-ADDR
                       SRC-UDP-PORT DST-IP-ADDR
       3) mirror <1-4> [ name NAME-STR ] remote ip SRC-IP-ADDR
                       SRC-UDP-PORT DST-IP-ADDR
       4) no mirror <1-4> [ name NAME-STR ]
       5) mirror endpoint ip SRC-IP-ADDR SRC-UDP-PORT DST-IP-ADDR
                        port PORT-NUM
       6) no mirror endpoint ip SRC-IP-ADDR SRC-UDP-PORT DST-IP-ADDR

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  o <1-4> - Mirror destination number
             o name NAME-STR - Friendly name to be associated with the
             mirror destionation number.
             o PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
             o SRC-IP-ADDR - source ip address for remote mirroring.
             o SRC-UDP-PORT - source UDP port for remote mirroring.
             o DST-IP-ADDR - destination ip address for remote mirroring.

Note1: The SRC-IP-ADDR, SRC-UDP-PORT, and DST_IP_ADDR specified on the
       source switch must match those on the respective destination switch.
Note2: The SRC-IP-ADDR, SRC-UDP-PORT, and DST-IP-ADDR must not be uses if the
       'no' keyword is used unless the 'endpoint' keyword is used.
```

Caution

A mirror exit port should be connected only to a network analyzer, IDS, or other network edge device that has no connection to other network resources. Allowing a mirror exit port connection to a network can result in serious network performance problems, and is strongly discouraged by ProCurve Networking.

COMMAND STRUCTURE

- [no] mirror **endpoint** -- Remote mirroring destination configuration. **(p. 253)**
  - **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 253)**
    - **mirror_session_ip_udp < 1 to 65535 >** -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 254)**

© 2007 Hewlett-Packard Development Company, L.P.

        - **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 254)**
            - **port** -- Remote mirroring destination port. ([ethernet] PORT-NUM) **(p. 255)**
- [no] mirror **mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 254)**
    - **name** -- Mirroring destination name string. (ASCII-STR) **(p. 255)**
        - **port** -- Mirroring destination monitoring port. ([ethernet] PORT-NUM) **(p. 255)**
        - **remote** -- Remote mirroring destination configuration. **(p. 255)**
            - **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 253)**
                - **mirror_session_src_udp < 1 to 65535 >** -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 254)**
                    - **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 254)**
    - **port** -- Mirroring destination monitoring port. ([ethernet] PORT-NUM) **(p. 255)**
    - **remote** -- Remote mirroring destination configuration. **(p. 255)**
        - **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 253)**
            - **mirror_session_src_udp < 1 to 65535 >** -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 254)**
                - **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 254)**
- [no] mirror **name** -- Mirror destination name. **(p. 255)**

COMMAND DETAILS

endpoint (p. 253)	**mirror_session_id (p. 254)**	**name (p. 255)**
ip (p. 253)	**mirror_session_ip_udp (p. 254)**	**port (p. 255)**
mirror_session_dest_ip (p. 254)	**mirror_session_src_udp (p. 254)**	**remote (p. 255)**

endpoint

- [no] mirror endpoint

```
Remote mirroring destination configuration.
```

Next Available Option:

- **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 253)**

ip

- mirror *< 1 to 4 >* name *NAME* remote ip *IP-ADDR*

```
Remote mirroring destination configuration.
```

Next Available Option:

- **mirror_session_src_udp** < 1 to 65535 > -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 254)**

- mirror *< 1 to 4 >* remote ip *IP-ADDR*

```
Remote mirroring destination configuration.
```

Next Available Option:

- **mirror_session_src_udp** < 1 to 65535 > -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 254)**

© 2007 Hewlett-Packard Development Company, L.P.

- [no] mirror endpoint ip *IP-ADDR*

  ```
  Remote mirroring destination configuration.
  ```

  Next Available Option:
  - **mirror_session_ip_udp** < 1 to 65535 > -- Remote mirroring UDP encapsulation port. (TCP/UDP-PORT) **(p. 254)**

mirror_session_dest_ip

- mirror *< 1 to 4 >* name *NAME* remote ip *IP-ADDR < 1 to 65535 > IP-ADDR*

  ```
  Remote mirroring UDP encapsulation destination ip addr.
  ```

- mirror *< 1 to 4 >* remote ip *IP-ADDR < 1 to 65535 > IP-ADDR*

  ```
  Remote mirroring UDP encapsulation destination ip addr.
  ```

- [no] mirror endpoint ip *IP-ADDR < 1 to 65535 > IP-ADDR*

  ```
  Remote mirroring UDP encapsulation destination ip addr.
  ```

  Next Available Option:
  - **port** -- Remote mirroring destination port. ([ethernet] PORT-NUM) **(p. 255)**

mirror_session_id

- [no] mirror *< 1 to 4 >*

  ```
  Mirror destination number.
  ```

  Range: < 1 to 4 >

  Next Available Options:
  - **name** -- Mirroring destination name string. (ASCII-STR) **(p. 255)**
  - **port** -- Mirroring destination monitoring port. ([ethernet] PORT-NUM) **(p. 255)**
  - **remote** -- Remote mirroring destination configuration.**(p. 255)**

mirror_session_ip_udp

- [no] mirror endpoint ip *IP-ADDR < 1 to 65535 >*

  ```
  Remote mirroring UDP encapsulation port.
  ```

  Range: < 1 to 65535 >

  Next Available Option:
  - **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 254)**

mirror_session_src_udp

- mirror *< 1 to 4 >* name *NAME* remote ip *IP-ADDR < 1 to 65535 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Remote mirroring UDP encapsulation port.
```

Range: < 1 to 65535 >

Next Available Option:
- **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 254)**

- mirror *< 1 to 4 >* remote ip *IP-ADDR < 1 to 65535 >*

```
Remote mirroring UDP encapsulation port.
```

Range: < 1 to 65535 >

Next Available Option:
- **mirror_session_dest_ip** -- Remote mirroring UDP encapsulation destination ip addr. (IP-ADDR) **(p. 254)**

name

- mirror *< 1 to 4 >* name *NAME*

```
Mirroring destination name string.
```

Next Available Options:
- **port** -- Mirroring destination monitoring port. ([ethernet] PORT-NUM) **(p. 255)**
- **remote** -- Remote mirroring destination configuration.**(p. 255)**

- [no] mirror name

```
Mirror destination name.
```

port

- mirror *< 1 to 4 >* name *NAME* port *[ETHERNET] PORT-NUM*

```
Mirroring destination monitoring port.
```

- mirror *< 1 to 4 >* port *[ETHERNET] PORT-NUM*

```
Mirroring destination monitoring port.
```

- mirror endpoint ip *IP-ADDR < 1 to 65535 > IP-ADDR* port *[ETHERNET] PORT-NUM*

```
Remote mirroring destination port.
```

remote

- mirror *< 1 to 4 >* name *NAME* remote

```
Remote mirroring destination configuration.
```

Next Available Option:
- **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 253)**

© 2007 Hewlett-Packard Development Company, L.P.

- mirror *< 1 to 4 >* remote

  ```
  Remote mirroring destination configuration.
  ```

  Next Available Option:
  - **ip** -- Remote mirroring destination configuration. (IP-ADDR) **(p. 253)**

mirror-port

OVERVIEW

Category:	config
Primary context:	config
Related Commands	vlan (page 457)

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

COMMAND STRUCTURE

- [no] mirror-port port_num -- Define the mirror port for diagnostic purposes ([ethernet] PORT-NUM) (p. 257)

EXAMPLES

Example: mirror-port

Assign port A6 as the monitoring port:

```
ProCurve(config)# mirror-port a6
```

COMMAND DETAILS

port_num (p. 257)

port_num

- [no] mirror-port *[ETHERNET] PORT-NUM*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
```

© 2007 Hewlett-Packard Development Company, L.P.

```
cannot be a trunked port. The parameter must be specified,
if the 'no' keyword is not used. Otherwise, it must not be
present.
```

© 2007 Hewlett-Packard Development Company, L.P.

module

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**show modules (page 366)**

```
Usage: module <MODULE-NUM>  module-type <MODULE-TYPE>

Description: Configure the type of module in a chassis slot.
```

COMMAND STRUCTURE

- module < 1 to 12 > **type < J8701A | J8702A | J8705A | ... >** -- The type of the module. **(p. 259)**

EXAMPLES

Example: module SLOT-NUM type MODULE-TYPE

Configure slot 4 for module type j4820a:

```
ProCurve(config)# module 4 type j4820a
```

COMMAND DETAILS

type (p. 259)

type

- module *< 1 to 12 >* type *< J8701A | J8702A | J8705A | ... >*

  ```
  The type of the module.
  ```

  Supported Values:
  - **J8701A**
  - **J8702A**
  - **J8705A**
  - **J8706A**
  - **J8707A**
  - **J8708A**
  - **J86yyA**
  - **J86xxA**
  - **J86yyA**
  - **J86xxA**
  - **J8694A**
  - **JFIXME**
  - **J90XXA**
  - **JXXXXA**
  - **JXXXXB**
  - **JXXXXA**
  - **J9051A**
  - **J9052A**
  - **No Blade Inserted**

© 2007 Hewlett-Packard Development Company, L.P.

page

OVERVIEW

Category:	CLI Setup
Primary context:	manager
Related Commands	

```
Usage: [no] page

Description: Toggle paging of the CLI display. When paging is enabled, printing
             of output is paused when a full page of text is displayed. When paging
             is disable, printing continues until the end of the output.
```

© 2007 Hewlett-Packard Development Company, L.P.

password

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**front-panel-security (page 147)** **show front-panel-security (page 350)**

```
Usage: [no] password <manager|operator> [user-name ASCII-STR]
       [no] password all

Description: Set or clear local password/username for manager and/or
             operator.
             Invoked without 'no', the command sets or changes existent
             password(s). The user will be prompted to enter the new
             password twice. The command removes local password protection,
             if preceded by 'no'.
Parameters:
    o <manager|operator|all> - Class of user. If 'all' is specified,
             the command applies to both manager and operator.
    o user-name ASCII-STR - Username (up to 15 characters) for manager
             or operator. Cannot be specified with 'all'.
```

COMMAND STRUCTURE

- [no] password **access < Manager | Operator >** -- Set or clear local password/username for manager and/or operator **(p. 261)**
  - **user-name** -- Set username for the specified user category. (ASCII-STR) **(p. 262)**
- [no] password **all < All >** -- Set or clear local password/username for manager and/or operator **(p. 262)**

EXAMPLES

COMMAND DETAILS

access (p. 261)	**all (p. 262)**	**user-name (p. 262)**

access

- [no] password *< Manager | Operator >*

```
Usage: [no] password <manager|operator> [user-name ASCII-STR]
       [no] password all

Description: Set or clear local password/username for manager and/or
             operator.
             Invoked without 'no', the command sets or changes existent
             password(s). The user will be prompted to enter the new
             password twice. The command removes local password protection,
             if preceded by 'no'.
Parameters:
    o <manager|operator|all> - Class of user. If 'all' is specified,
             the command applies to both manager and operator.
    o user-name ASCII-STR - Username (up to 15 characters) for manager
             or operator. Cannot be specified with 'all'.
```

© 2007 Hewlett-Packard Development Company, L.P.

Supported Values:
- **Manager** -- Configure manager access.
- **Operator** -- Configure operator access.

Next Available Option:
- **user-name** -- Set username for the specified user category. (ASCII-STR) **(p. 262)**

all

- [no] password *< All >*

```
Usage: [no] password <manager|operator> [user-name ASCII-STR]
       [no] password all

Description: Set or clear local password/username for manager and/or
             operator.
             Invoked without 'no', the command sets or changes existent
             password(s). The user will be prompted to enter the new
             password twice. The command removes local password protection,
             if preceded by 'no'.
Parameters:
    o <manager|operator|all> - Class of user. If 'all' is specified,
             the command applies to both manager and operator.
    o user-name ASCII-STR - Username (up to 15 characters) for manager
             or operator. Cannot be specified with 'all'.
```

Supported Values:
- **All** -- Configure both, manager and operator access.

user-name

- password *< Manager | Operator >* user-name *USER-NAME*

```
Set username for the specified user category.
```

© 2007 Hewlett-Packard Development Company, L.P.

ping

OVERVIEW

Category:	
Primary context:	operator
Related Commands	**traceroute (page 448)** **link-test (page 229)**

```
Usage: ping <IP-ADDR | hostname | SWITCH-NUM>
            [repetitions <1-10000>] [timeout <1-60>]
            [data-size <0-65507>] [data-fill <0-1024>]

Description: Send IP Ping requests to a device on the network.

Parameters:

   o IP-ADDR    - Network IP address of station to which to send IP Ping.

   o hostname   - domain name of station to which to send IP Ping.

   o SWITCH-NUM - The number of Stack member switch (1..16)

   o [repetitions <1-10000>] - Number of times to send IP Ping; the default
     value is 1.

   o [timeout <1-60>] - Seconds within which a response is required

   o [data-size <0-65507>] - Size of the data to be sent; the default
     size is 0.

   o [data-fill <0-1024>] - The string to be filled in the data portion
     of the packet. A string upto 1024 characters in length can be
     specified. The default value is a 0 length string.
```

COMMAND STRUCTURE

- ping **data-fill** -- Ping data fill string (size <0-1024>). (OCTET-STR) **(p. 264)**
- ping **data-size < 0 to 65507 >** -- Ping data size <0-65507>. (NUMBER) **(p. 264)**
- ping **host-name** -- Domain name of the host to ping. (ASCII-STR) **(p. 264)**
- ping **ip-addr** -- IP address to ping. (IP-ADDR) **(p. 264)**
- ping **repetitions < 1 to 10000 >** -- Number of packets to send <1-10000>. (NUMBER) **(p. 264)**
- ping **switch-num** -- The number of Stack member switch to ping. (NUMBER) **(p. 264)**
- ping **timeout < 1 to 60 >** -- Ping timeout in seconds <1-60>. (NUMBER) **(p. 264)**

EXAMPLES

Example: ping IP-ADDR

Send an IP Ping request to the device that has IP address 10.10.10.1:

```
ProCurve# ping 10.10.10.1
10.10.10.1 is alive, time = 50 ms
```

© 2007 Hewlett-Packard Development Company, L.P.

COMMAND DETAILS

data-fill (p. 264)	ip-addr (p. 264)	timeout (p. 264)
data-size (p. 264)	repetitions (p. 264)	
host-name (p. 264)	switch-num (p. 264)	

data-fill

- ping data-fill *OCTET-STR*

```
Ping data fill string (size <0-1024>).
```

data-size

- ping data-size *< 0 to 65507 >*

```
Ping data size <0-65507>.
```

Range: < 0 to 65507 >

host-name

- ping *HOST-NAME*

```
Domain name of the host to ping.
```

ip-addr

- ping *IP-ADDR*

```
IP address to ping.
```

repetitions

- ping repetitions *< 1 to 10000 >*

```
Number of packets to send <1-10000>.
```

Range: < 1 to 10000 >

switch-num

- ping *NUMBER*

```
The number of Stack member switch to ping.
```

timeout

- ping timeout *< 1 to 60 >*

```
Ping timeout in seconds <1-60>.
```

Range: < 1 to 60 >

© 2007 Hewlett-Packard Development Company, L.P.

port-security

OVERVIEW

Category:	Port Security
Primary context:	config
Related Commands	**show port-security (page 373)** **show mac-address (page 364)**

```
Usage: [no] port-security [ethernet] PORT-LIST
          [learn-mode <continuous|static|configured|
                       limited-continuous|port-access>]
          [address-limit <1-32>]
          [mac-address MAC-ADDR [MAC-ADDR ...]]
          [action <none|send-alarm|send-disable>]
          [clear-intrusion-flag]

Description: Set the port-security operation(s) for each port in port list.

Parameters:

    o learn-mode <continuous|static|configured|limited-continuous|port-access>
             If 'continuous' is specified, the port continually learns new
             addresses on the port. If 'static' is specified, the user
             can configure addresses that are authorized to use on that port
             and let the switch learn the remaining addresses up to the
             specified address-limit. If 'configured' is specified, up
             to address-limit configured addresses are authorized. Use the
             'address-limit' parameter to specify the maximum number of
             static addresses for the port.
             The 'port-access' instructs the device to learn only the MAC
             addresses authorized by 802.1x or Web/MAC authentication
             subsystem. After a MAC address is authorized, only traffic
             from the authorized MAC address is allowed.
             If 'limited-continuous' is specified, the first
             'address-limit' source MAC addresses heard on this
             port become the authorized addresses. When new authorized
             addresses are learned, they are stored in a table. When
             the table has reached its 'address-limit', any
             new source MAC addresses received on the port
             constitutes an intrusion. The authorized addresses in
             this mode will age out of the system, therefore the
             list of authorized addresses can be dynamic over time.
    o address-limit <1-N> - This parameter is valid only when the learn-mode
             is static, configured, or limited-continuous.
             It defines the number of MAC address that the table for the
             given port will hold. For static and configured N is equal
             to 8. For limited-continuous N is equal to 32.
    o mac-address MAC-ADDR ... - This 12-hex digit parameter is only valid
             when the learn-mode is static. The parameter is used to configure
             the addresses that are authorized to use the port. The maximum
             number of authorized addresses that may be configured and
             learned is 8. If the number of configured addresses is less
             than the address-limit, the switch will learn the remaining
             number of addresses. Several addresses can be specified in
             one command line.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
o action <none|send-alarm|send-disable> - Indicates the port security
         action the switch will take if an intruder is detected on the
         port.
o clear-intrusion-flag - clears intrusion indicator for the ports
         specified in the command PORT-LIST.
```

COMMAND STRUCTURE

- port-security [ETHERNET] PORT-LIST **action < none | send-alarm | send-disable >** -- Define device's action in case of an intrusion detection. **(p. 266)**
- port-security [ETHERNET] PORT-LIST **address-limit < 1 to 32 >** -- Define number of authorized addresses on the port(s). **(p. 267)**
- port-security [ETHERNET] PORT-LIST **clear-intrusion-flag** -- Clear intrusion indicator for the port(s) **(p. 267)**
- port-security [ETHERNET] PORT-LIST **learn-mode < continuous | static | configured | ... >** -- Define the mode of acquiring authorized MAC address(es). **(p. 267)**
- [no] port-security [ETHERNET] PORT-LIST **mac-address** -- Configure the address(es) authorized on the port(s). **(p. 267)**
  - **mac-addr** -- Authorized MAC address. (MAC-ADDR) **(p. 267)**

EXAMPLES

Example: port-security learn-mode

Configure port A1 to automatically accept the first device (MAC address) it detects as the only authorized device for that port. (The default device limit is 1.) This command also configures the port to send an alarm to a network management station and disable itself if an intruder is detected on the port.

```
ProCurve(config)# port-security a1 learn-mode static action send-disable
```

Example: port-security learn-mode

Configure port A5 to allow two MAC addresses, 00c100-7fec00 and 0060b0-889e00, as the authorized devices. This command also configures the switch to send an alarm to a management station if an intruder is detected on the port, but nonetheless to allow the intruder to access to the network.

```
ProCurve(config)# port-security a5 learn-mode static
address-limit 2 mac-address 00c100-7fec00 0060b0-889e00
action send-alarm
```

COMMAND DETAILS

action (p. 266)	**clear-intrusion-flag (p. 267)**	**mac-addr (p. 267)**
address-limit (p. 267)	**learn-mode (p. 267)**	**mac-address (p. 267)**

action

- port-security *[ETHERNET] PORT-LIST* action *< none | send-alarm | send-disable >*

```
Define device's action in case of an intrusion detection.
```

Supported Values:
- **none**
- **send-alarm**
- **send-disable**

© 2007 Hewlett-Packard Development Company, L.P.

address-limit

- port-security *[ETHERNET] PORT-LIST* address-limit *< 1 to 32 >*

```
Define number of authorized addresses on the port(s).
```

Range: < 1 to 32 >

clear-intrusion-flag

- port-security *[ETHERNET] PORT-LIST* clear-intrusion-flag

```
Clear intrusion indicator for the port(s)
```

learn-mode

- port-security *[ETHERNET] PORT-LIST* learn-mode *< continuous | static | configured | ... >*

```
Define the mode of acquiring authorized MAC address(es).
```

Caution

Using the "static" parameter with a device limit greater than the number of MAC addresses specified with "mac-address" can allow an unwanted device to become "authorized". This is because the port, to fulfill the number of devices allowed by the "address-limit" parameter, automatically adds devices it detects until it reaches the specified limit.

Supported Values:

- **continuous** -- Continuous MAC address learn mode.
- **static** -- Static MAC address learn mode.
- **configured** -- Static MAC address configured mode.
- **port-access** -- Learn port-access authorized MAC address only.
- **limited-continuous** -- Limited continuous MAC address learn mode.

mac-addr

- port-security *[ETHERNET] PORT-LIST* mac-address *MAC-ADDR*

```
Authorized MAC address.
```

mac-address

- [no] port-security *[ETHERNET] PORT-LIST* mac-address

```
Configure the address(es) authorized on the port(s).
```

Next Available Option:

- **mac-addr** -- Authorized MAC address. (MAC-ADDR) **(p. 267)**

© 2007 Hewlett-Packard Development Company, L.P.

power

OVERVIEW

Category:	Power
Primary context:	config
Related Commands	**show power-management (page 374)**

```
Usage: power [slot <SLOT-LIST>] [threshold <1-99>][optional-parameters]

Description: Change the threshold for sending a power usage change notification. The
             switch sends a notification when the power usage on a PoE module either
             exceeds or drops below the threshold. The threshold is a percentage
             of the power available on the module. Default threshold: 80%
             threshold - Set the power consumption percentage at which a
                         trap should be sent.
             optional-parameters - Use <TAB> or <?> after entering power
                         to see a list of all available options.
```

COMMAND STRUCTURE

- [no] power **pre-std-detect** -- Detect and power pre-802 **(p. 268)**
- power **slot** -- Optional - Specify a valid powered-slot list for power threshold setting or omit to set all powered-slots. (SLOT-ID-RANGE) **(p. 268)**
  - **threshold < 1 to 99 >** -- Set the power consumption percentage at which a trap should be sent. (NUMBER) **(p. 268)**
- power **threshold < 1 to 99 >** -- Set the power consumption percentage at which a trap should be sent. (NUMBER) **(p. 268)**

COMMAND DETAILS

pre-std-detect (p. 268)	**slot (p. 268)**	**threshold (p. 268)**

pre-std-detect

- [no] power pre-std-detect

```
Usage: [NO] power pre-std-detect

Description: Detect and power pre-802.3af-standard devices.
```

slot

- power slot *SLOT-ID-RANGE*

```
Optional - Specify a valid powered-slot list for power threshold setting or
           omit to set all powered-slots.
```

Next Available Option:

- **threshold** < 1 to 99 > -- Set the power consumption percentage at which a trap should be sent. (NUMBER) **(p. 268)**

threshold

- power threshold *< 1 to 99 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Set the power consumption percentage at which a trap should be sent.
```

Range: < 1 to 99 >

- power slot *SLOT-ID-RANGE* threshold *< 1 to 99 >*

```
Set the power consumption percentage at which a trap should be sent.
```

Range: < 1 to 99 >

© 2007 Hewlett-Packard Development Company, L.P.

primary-vlan

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**show vlan (page 390)**

```
Usage: primary-vlan VLAN-ID

Description: Set the VLAN that is to be used as the primary VLAN.
             The primary VLAN is used by stacking, DHCP, and TIMEP.
             The default primary VLAN is VLAN 1 (DEFAULT_VLAN).
```

EXAMPLES

Example: primary-vlan VLAN-ID

Reassign the Primary VLAN and change the VLAN name:

```
HPswitch(config)# primary-vlan 22
HPswitch(config)# vlan 22 name 22-Primary
HPswitch(config)# show vlans

 Status and Counters - VLAN Information

  Maximum VLANs to support : 8
  Primary VLAN : 22-Primary
  Management VLAN :

  802.1Q VLAN ID Name          Status      Voice  Jumbo
  -------------- ------------- ----------- -----  -----
  1              DEFAULT_VLAN  Static      No     No
  22             22-Primary    Static      No     No
```

print

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: print COMMAND-STR

Description: Execute a command and redirect its output to the device channel
             for current session.
```

COMMAND STRUCTURE

- print **command** -- Command to execute. Use quotes for multiword commands. (ASCII-STR) **(p. 271)**

COMMAND DETAILS

command (p. 271)

command

- print *COMMAND*

```
Command to execute. Use quotes for multiword commands.
```

© 2007 Hewlett-Packard Development Company, L.P.

qos

OVERVIEW

Category:	QoS
Primary context:	config
Related Commands	**show qos (page 374)**

```
Usage: [no] qos ...

Description: Configure Quality of Service (QoS) on the device. The
             command must be followed by a keyword defining a subdomain
             of the QoS parameters to configure.
```

COMMAND STRUCTURE

- [no] qos **apptype < udp-port | tcp-port >** -- Configure priorities for TCP/UDP services **(p. 273)**
  - **port-num** -- TCP/UDP port from [to] which to prioritize traffic. (TCP/UDP-PORT) **(p. 277)**
    - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 275)**
    - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 278)**
- [no] qos **device-priority** -- Configure device-based priority (IP-ADDR) **(p. 275)**
  - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 275)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 278)**
- [no] qos **dscp-map < 000000 | 000001 | 000010 | ... >** -- Define mapping between a DSCP (Differentiated-Services Codepoint) value and an 802 **(p. 276)**
  - **name** -- Specify DSCP->priority mapping name. **(p. 277)**
    - **name-string** -- Specify DSCP->priority mapping name. (ASCII-STR) **(p. 277)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 278)**
- [no] qos **protocol < IP | IPX | ARP | ... >** -- Configure protocol-based priority **(p. 278)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 278)**
- qos **queue-config** -- Sets the number of outbound port queues that buffer the packets depending on their 802 **(p. 279)**
  - **2-queues** -- Set the number of outbound port queues for all switch ports. **(p. 273)**
  - **4-queues** -- Set the number of outbound port queues for all switch ports. **(p. 273)**
  - **8-queues** -- Set the number of outbound port queues for all switch ports. **(p. 273)**
- [no] qos **type-of-service** -- Configure the Type-of-Service method the device uses to prioritize IP traffic **(p. 280)**
  - **diff-services** -- In IP Differentiated Services (Diffserv) mode, IPv4 packets are classified and given a QoS priority based on the upper 6 bits of the IP ToS field from the packets as they enter the switch. The assignment of Diffserv Codepoints to 802.1p priorities is done via the qos dscp-map command. Any Diffserv Codepoint in an inbound IPv4 packet can be re-mapped to a different codepoint (and its associated 802.1p priority) on outbound. This is done by using the syntax: qos type-of-service diff-services <000000...111111> dscp <000000..111111> **(p. 275)**
    - **codepoint < 000000 | 000001 | 000010 | ... >** -- Configure the Type-of-Service method the device uses to prioritize IP traffic **(p. 273)**
      - **dscp < 000000 | 000001 | 000010 | ... >** -- Define Differentiated Services Codepoint to which to map IP ToS. **(p. 275)**
  - **ip-precedence** -- In IP-Precedence mode, IPv4 packets are classified and given a QoS priority based on the upper 3 bits of the IP ToS field. The priority association is automatic and cannot be changed: IP-Precedence 802.1p ToS Bits Priority ---------- 111 7 (Highest) 110 6 101 5 100 4 011 3 010 0 (Normal) 001 2 (Low) 000 1 (Lowest) **(p. 277)**

© 2007 Hewlett-Packard Development Company, L.P.

COMMAND DETAILS

2-queues (p. 273)	diff-services (p. 275)	port-num (p. 277)
4-queues (p. 273)	dscp (p. 275)	priority (p. 278)
8-queues (p. 273)	dscp-map (p. 276)	protocol (p. 278)
apptype (p. 273)	ip-precedence (p. 277)	queue-config (p. 279)
codepoint (p. 273)	name (p. 277)	type-of-service (p. 280)
device-priority (p. 275)	name-string (p. 277)	

2-queues

- qos queue-config 2-queues

```
Set the number of outbound port queues for all switch ports.
```

4-queues

- qos queue-config 4-queues

```
Set the number of outbound port queues for all switch ports.
```

8-queues

- qos queue-config 8-queues

```
Set the number of outbound port queues for all switch ports.
```

apptype

- [no] qos *< udp-port | tcp-port >*

```
Usage: [no] qos <udp|tcp> TCP/UDP-PORT [dscp <000000|000001...111111>|
                                        priority <0-7>]

Description: Configure priorities for TCP/UDP services. The priority can
             be defined for packets sourced and destined to a particular
             TCP/UDP service. The specified priority value will be placed
             in the 802.1p priority field of outgoing tagged packets. The
             packets will also be placed in the appropriate outbound priority
             queue. '7' means highest priority.  If 'dscp' is specified, the
             priority of the outgoing packets is defined by the
             Differentiated Services Codepoint mapping (see 'show qos
             dscp-map'). Using 'no' removes any priority assignment for
             this TCP/UDP service.
```

Supported Values:

- **udp-port** -- Set UDP port based priority.
- **tcp-port** -- Set TCP port based priority.

Next Available Option:

- **port-num** -- TCP/UDP port from [to] which to prioritize traffic. (TCP/UDP-PORT) **(p. 277)**

codepoint

- [no] qos type-of-service diff-services *< 000000 | 000001 | 000010 | ... >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] type-of-service <ip-precedence|
                             diff-services <000000|000001...111111>
                             [dscp <000000|000001...111111>]>

Description: Configure the Type-of-Service method the device uses to
             prioritize IP traffic.  Prioritization is done based on the
             contents of the Type of Service (ToS) field in the IP header
             of each packet.  Using 'no' type-of-service with just the
             mode (ip-precedence or diff-services) will disable all ToS
             QoS for the switch.

Modes:
--------------
Disabled        The switch does NOT prioritize IP packets based on the IP
                ToS field.

IP Precedence   The switch uses the upper 3 bits of the IP ToS field (the IP
                Precedence bits) to determine the 802.1p priority of the
                packet and its outbound switch queue. If the packet is
                transmitted out a port on which VLAN tagging is enabled, the
                new priority is placed in the outbound VLAN tag. See the
                switch documentation for more information.

Differentiated  The switch uses the upper 6 bits of the ToS field (the
Services        Differentiated Services bits) to decide whether to apply an
                802.1p priority to the packet and thus affect its outbound
                queue. The priority is defined by the Differentiated
                Services Codepoint mapping (see 'show qos dscp-map'). If no
                priority is mapped for the packet's codepoint, the switch
                does not classify the packet using Differentiated Services.
                If there IS an associated priority configured, and the
                packet is transmitted out a port on which VLAN tagging is
                enabled, the new 802.1p priority will be placed in the
                outbound VLAN tag.  If a DSCP Policy is configured to apply
                to the inbound DS codepoint (i.e., the codepoint has been
                're-mapped'), the priority assignment and outbound queueing
                will be that specified by the new Policy's codepoint in the
                DSCP table, and the Differentiated Services field in the
                outbound packet will be changed to the new value.
                Using 'no type-of-service diff-services <000000...111111>'
                removes the re-mapping assignment, i.e., a new DSCP Policy
                will no longer be applied to the specified codepoint. To
                remove a priority association from a codepoint altogether,
                the  'no dscp-map <000000.111111>' function must be used.

    o diff-services <000000|000001...111111> - The value of the upper
      6 bits in the ToS field.

    o dscp <000000|000001...111111> - Re-maps a given inbound Differentiated
      Services codepoint to the specified DSCP Policy and codepoint on
      outbound.
```

Supported Values:

Binary formatted value from 000000 to 111111

Next Available Option:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Define Differentiated Services Codepoint to which to map IP ToS.**(p. 275)**

© 2007 Hewlett-Packard Development Company, L.P.

device-priority

- [no] qos device-priority *IP-ADDR*

```
Usage: [no] qos device-priority IP-ADDR [dscp <000000|000001...111111>|
                                         priority <0-7>]

Description: Configure device-based priority. The priority can be set for
             IP packets from/to a particular IP Address.  The specified
             priority value will be placed in the 802.1p priority field of
             outgoing tagged packets. The packets will also be placed in
             the appropriate outbound priority queue. '7' means highest
             priority. If 'dscp' is specified, the priority of the outgoing
             packets is defined by the Differentiated Services Codepoint
             mapping (see 'show qos dscp-map').  Using 'no' removes any
             priority assignment for this IP address.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 275)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 278)**

diff-services

- qos type-of-service diff-services

```
In IP Differentiated Services (Diffserv) mode, IPv4 packets are classified
      and given a QoS priority based on the upper 6 bits of the IP ToS
      field from the packets as they enter the switch.

      The assignment of Diffserv Codepoints to 802.1p priorities is done
      via the qos dscp-map command.

      Any Diffserv Codepoint in an inbound IPv4 packet can be re-mapped to
      a different codepoint (and its associated 802.1p priority) on
      outbound. This is done by using the syntax:

      qos type-of-service diff-services <000000...111111> dscp <000000..111111>
```

Next Available Option:

- **codepoint** < 000000 | 000001 | 000010 | ... > -- Configure the Type-of-Service method the device uses to prioritize IP traffic**(p. 273)**

dscp

- qos device-priority *IP-ADDR* dscp *< 000000 | 000001 | 000010 | ... >*

```
Specify DSCP policy to use.
```

Supported Values:

Binary formatted value from 000000 to 111111

- qos *< udp-port | tcp-port > TCP/UDP-PORT* dscp *< 000000 | 000001 | 000010 | ... >*

```
Specify DSCP policy to use.
```

© 2007 Hewlett-Packard Development Company, L.P.

Supported Values:

Binary formatted value from 000000 to 111111

- qos type-of-service diff-services *< 000000 | 000001 | 000010 | ... >* dscp *< 000000 | 000001 | 000010 | ... >*

```
Define Differentiated Services Codepoint to which to map IP ToS.
```

Supported Values:

Binary formatted value from 000000 to 111111

dscp-map

- [no] qos dscp-map *< 000000 | 000001 | 000010 | ... >*

```
Usage: [no] qos dscp-map <000000|000001...111111>
                         [priority <<0-7>|no-override>]
                         [name <str>]

Description: Define mapping between a DSCP (Differentiated-Services
             Codepoint) value and an 802.1p priority. The mapping is used
             to assign priority for IPv4 packets if a QoS classifier uses
             this DSCP policy as the method of traffic prioritization.

            The mapping also provides the profile for inbound classification
            and priority assignment based on an IPv4 packet's received
            IP ToS byte ONLY IF the user has also configured
                 'qos type-of-service diff-services'

             'no qos dscp-map <codepoint>' will remove the settings for the
             specified codepoint from the running configuration.  The
             priority is set to no-override and the name is deleted (the
             priority and name can only be removed if no QoS feature is
             configured to use this DSCP Policy).
             'no qos dscp-map <codepoint> name'  will remove the name
             associated with this policy, but not the policy priority.

             Certain codepoints may have a default associated 802.1p
             priority, as part of the IETF standards for Assured Forwarding
             and Expedited Forwarding. These are automatically configured as
             follows:

                DiffServ       802.1p
                Codepoint       Value       IETF Standard Designation
                ------------------------------------------------------
                001010            1         Assured Forwarding   AF11
                001100            1         Assured Forwarding   AF12
                001110            2         Assured Forwarding   AF13
                010010            0         Assured Forwarding   AF21
                010100            0         Assured Forwarding   AF22
                010110            3         Assured Forwarding   AF23
                011010            4         Assured Forwarding   AF31
                011100            4         Assured Forwarding   AF32
                011110            5         Assured Forwarding   AF33
                100010            6         Assured Forwarding   AF41
                100100            6         Assured Forwarding   AF42
                100110            7         Assured Forwarding   AF43
                101110            7         Expedited Forwarding EF
```

© 2007 Hewlett-Packard Development Company, L.P.

Supported Values:

Binary formatted value from 000000 to 111111

Next Available Options:
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 278)**
- **name** -- Specify DSCP->priority mapping name. **(p. 277)**

ip-precedence

- qos type-of-service ip-precedence

```
In IP-Precedence mode, IPv4 packets are classified and given a QoS priority
      based on the upper 3 bits of the IP ToS field. The priority
      association is automatic and cannot be changed:
             IP-Precedence      802.1p
               ToS Bits        Priority
             --------------------------------
                111               7 (Highest)
                110               6
                101               5
                100               4
                011               3
                010               0 (Normal)
                001               2 (Low)
                000               1 (Lowest)
```

name

- [no] qos dscp-map *< 000000 | 000001 | 000010 | ... >* name

```
Specify DSCP->priority mapping name.
```

Next Available Option:
- **name-string** -- Specify DSCP->priority mapping name. (ASCII-STR) **(p. 277)**

name-string

- qos dscp-map *< 000000 | 000001 | 000010 | ... >* name *NAME-STRING*

```
Specify DSCP->priority mapping name.
```

port-num

- qos *< udp-port | tcp-port > TCP/UDP-PORT*

```
TCP/UDP port from [to] which to prioritize traffic.
```

Next Available Options:
- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 275)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 278)**

© 2007 Hewlett-Packard Development Company, L.P.

priority

- qos device-priority *IP-ADDR* priority *< 0 | 1 | 2 | ... >*

  Specify priority to use.

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**
  - **7**
- qos dscp-map *< 000000 | 000001 | 000010 | ... >* priority *< 0 | 1 | 2 | ... >*

  Specify priority to use.

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**
  - **7**
- qos protocol *< IP | IPX | ARP | ... >* priority *< 0 | 1 | 2 | ... >*

  Specify priority to use.

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**
  - **7**
- qos *< udp-port | tcp-port > TCP/UDP-PORT* priority *< 0 | 1 | 2 | ... >*

  Specify priority to use.

  Supported Values:
  - **0**
  - **1**
  - **2**
  - **3**
  - **4**
  - **5**
  - **6**
  - **7**

protocol

- [no] qos protocol *< IP | IPX | ARP | ... >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] qos protocol <ip|ipx|arp|appletalk|sna|netbeui>
                         [priority <0-7>]

Description: Configure protocol-based priority. The priority can be
             defined for any of the listed protocol types. The specified
             priority value will be placed in the 802.1p priority field of
             outgoing tagged packets. The protocol packets will also be
             placed in the appropriate outbound priority queue. '7' means
             highest priority. Using 'no' removes any priority assignment
             for the specified protocol.
```

Supported Values:

- **IP**
- **IPX**
- **ARP**
- **AppleTalk**
- **SNA**
- **NetBEUI**

Next Available Option:

- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 278)**

queue-config

- qos queue-config

```
Usage: queue-config <2-queues|4-queues|8-queues>

Description: Sets the number of outbound port queues that buffer the
             packets depending on their 802.1p priority.  This command will
             execute a 'write memory', replacing the Startup configuration
             with the contents of the current Running configuration. The new
             configuration will reset the number of outbound port queues and
             remove any previously configured 'bandwidth-min output' settings.
             After the write memory is executed, the switch will reboot
             immediately.
             The mapping of 802.1p priorities to outbound port queues is
             shown below:

              802.1p
             Priority     | 2-queues | 4-queues | 8-queues
             ------------------------------------------
             1 (lowest)   |    1     |    1          1
             2            |    1     |    1          2
             0 (normal)   |    1     |    2          3
             3            |    1     |    2          4
             4            |    2     |    3          5
             5            |    2     |    3          6
             6            |    2     |    4          7
             7 (highest)  |    2     |    4          8
```

Next Available Options:

- **2-queues** -- Set the number of outbound port queues for all switch ports. **(p. 273)**
- **4-queues** -- Set the number of outbound port queues for all switch ports. **(p. 273)**
- **8-queues** -- Set the number of outbound port queues for all switch ports. **(p. 273)**

© 2007 Hewlett-Packard Development Company, L.P.

type-of-service

- [no] qos type-of-service

```
Usage: [no] type-of-service <ip-precedence|
                             diff-services <000000|000001...111111>
                             [dscp <000000|000001...111111>]>

Description: Configure the Type-of-Service method the device uses to
             prioritize IP traffic.  Prioritization is done based on the
             contents of the Type of Service (ToS) field in the IP header
             of each packet.  Using 'no' type-of-service with just the
             mode (ip-precedence or diff-services) will disable all ToS
             QoS for the switch.

Modes:
--------------
Disabled        The switch does NOT prioritize IP packets based on the IP
                ToS field.

IP Precedence   The switch uses the upper 3 bits of the IP ToS field (the IP
                Precedence bits) to determine the 802.1p priority of the
                packet and its outbound switch queue. If the packet is
                transmitted out a port on which VLAN tagging is enabled, the
                new priority is placed in the outbound VLAN tag. See the
                switch documentation for more information.

Differentiated  The switch uses the upper 6 bits of the ToS field (the
Services        Differentiated Services bits) to decide whether to apply an
                802.1p priority to the packet and thus affect its outbound
                queue. The priority is defined by the Differentiated
                Services Codepoint mapping (see 'show qos dscp-map'). If no
                priority is mapped for the packet's codepoint, the switch
                does not classify the packet using Differentiated Services.
                If there IS an associated priority configured, and the
                packet is transmitted out a port on which VLAN tagging is
                enabled, the new 802.1p priority will be placed in the
                outbound VLAN tag.  If a DSCP Policy is configured to apply
                to the inbound DS codepoint (i.e., the codepoint has been
                're-mapped'), the priority assignment and outbound queueing
                will be that specified by the new Policy's codepoint in the
                DSCP table, and the Differentiated Services field in the
                outbound packet will be changed to the new value.
                Using 'no type-of-service diff-services <000000...111111>'
                removes the re-mapping assignment, i.e., a new DSCP Policy
                will no longer be applied to the specified codepoint. To
                remove a priority association from a codepoint altogether,
                the  'no dscp-map <000000.111111>' function must be used.

    o diff-services <000000|000001...111111> - The value of the upper
      6 bits in the ToS field.

    o dscp <000000|000001...111111> - Re-maps a given inbound Differentiated
      Services codepoint to the specified DSCP Policy and codepoint on
      outbound.
```

Next Available Options:

- **ip-precedence** -- In IP-Precedence mode, IPv4 packets are classified and given a QoS priority based on the upper 3 bits of the IP ToS field. The priority association is automatic and cannot be changed:

© 2007 Hewlett-Packard Development Company, L.P.

IP-Precedence 802.1p ToS Bits Priority ---------- 111 7 (Highest) 110 6 101 5 100 4 011 3 010 0 (Normal) 001 2 (Low) 000 1 (Lowest)

(p. 277)

- **diff-services** -- In IP Differentiated Services (Diffserv) mode, IPv4 packets are classified and given a QoS priority based on the upper 6 bits of the IP ToS field from the packets as they enter the switch. The assignment of Diffserv Codepoints to 802.1p priorities is done via the qos dscp-map command. Any Diffserv Codepoint in an inbound IPv4 packet can be re-mapped to a different codepoint (and its associated 802.1p priority) on outbound. This is done by using the syntax: qos type-of-service diff-services <000000...111111> dscp <000000..111111> (p. 275)

© 2007 Hewlett-Packard Development Company, L.P.

radius-server

OVERVIEW

Category:	Switch Security
Primary context:	config
Related Commands	**show radius (page 375)**

```
Usage:   [no] radius-server host IP-ADDR [auth-port UDP-PORT]
                                         [acct-port UDP-PORT]
                                         [key KEY-STR]
         [no] radius-server key KEY-STR
              radius-server timeout <1-15>
              radius-server retransmit <1-5>
         [no] radius-server dead-time <1-1440>

Description: Configure RADIUS parameters.
             The first command adds/removes a RADIUS server to/from the
             list of the RADIUS servers that will be used for the
             authentication. Up to 3 RADIUS servers can be configured.
             The second command sets/removes the global encryption key used
             for RADIUS authentication.
             The third command sets the interval in seconds the switch
             waits for a reply from a RADIUS server.
             The fourth command specifies the number of times the switch
             retransmits requests to a RADIUS server.
             The last command sets the length of time in minutes a RADIUS
             server that failed to respond to an authentication request is
             bypassed by additional requests. See 'dead-time', below. Use
             the 'no' form of command to set the dead-time to 0.

Parameters:

    o host IP-ADDR [auth-port UDP-PORT] [acct-port UDP-PORT]
                   [key KEY-STR] - specifies
               the IP address of the RADIUS server to use. Optional parameter
               'auth-port UDP-PORT' specifies the UDP destination port
               used for authentication requests to the server (default
               is 1812).Optional parameter 'acct-port UDP-PORT' specifies
               the UDP destination port used for accounting requests to the
               server (default is 1813). Optional parameter 'key KEY-STR'
               specifies an encryption key used for authentication with the
               given server. The default is NULL. Specifying this key
               overrides the key set for this server by the global
               configuration 'radius-server key KEY-STR' command.
    o key KEY-STR - specifies the global encryption key, which is
               used for authentication if encryption key for the server is
               not configured. The default is NULL.
    o timeout <1-15> - server response timeout interval in seconds. The
               default is 5 seconds.
    o retransmit <1-5> - specifies the maximum number of retransmission
               attempts. The default is 3 attempts.
    o dead-time <1-1440> - If the switch does not receive a response from a
               specific RADIUS server, the switch avoids sending any new
               authentication requests to that server until the dead-time has
               expired. That is, during a new authentication attempt, the
```

© 2007 Hewlett-Packard Development Company, L.P.

```
switch bypasses a specified RADIUS server if a dead-time
period is running on the switch for a previous failure to
receive a response from that server. (The switch will still
send new authentication requests to any other configured
RADIUS servers that are not affected by a dead-time
condition.) For a specific RADIUS server, dead-time counting
begins with the end of the last timeout in the last retransmit
attempt of the failed authentication session. When dead-time
is set to 0 (zero), there is no dead-time and the switch will
not bypass a RADIUS server that has failed to respond to an
earlier authentication attempt. (Default: 0.)
```

COMMAND STRUCTURE

- [no] radius-server **dead-time < Min | Max >** -- Server unavailability time (default is 0, use the 'no' form of command to set the dead-time to 0). **(p. 285)**
  - **dead-time < 1 to 1440 >** -- Server unavailability time (default is 0, use the 'no' form of command to set the dead-time to 0). **(p. 285)**
- [no] radius-server **host** -- IP address of the RADIUS server to use. (IP-ADDR) **(p. 285)**
  - **acct-port** -- Accounting UDP destination port number (default is 1813). **(p. 284)**
    - **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 284)**
      - **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 284)**
      - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 285)**
  - **auth-port** -- Authentication UDP destination port number (default is 1812). **(p. 284)**
    - **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 284)**
      - **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 284)**
      - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 285)**
  - **key** -- Encryption key to use with the RADIUS server (default is NULL). **(p. 285)**
    - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 285)**
      - **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 284)**
      - **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 284)**
- [no] radius-server **key** -- Global encryption key (default is NULL). **(p. 285)**
  - **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 285)**
- radius-server **retransmit < 1 to 5 >** -- Number of packet retransmits (default is 3). **(p. 286)**
- radius-server **timeout < 1 to 15 >** -- Server timeout interval (default is 5). **(p. 286)**

EXAMPLES

Example: radius-server host

Configure the switch to access a RADIUS server at IP address 192.168.32.11 using a server-specific shared secret key of '1A7rd':

© 2007 Hewlett-Packard Development Company, L.P.

```
HP ProCurve Switch 5308xl(config)# radius-server host 192.168.32.11
HP ProCurve Switch 5308xl(config)# radius-server host 192.168.32.11 key 1A7rd

HP ProCurve Switch 5308xl(config)# show radius

 Status and Counters - General RADIUS Information

  Deadtime(min) : 0
  Timeout(secs) : 5
  Retransmit Attempts : 3
  Global Encryption Key :

                  Auth  Acct
  Server IP Addr  Port  Port  Encryption Key
  --------------- ----- ----- ---------------------------------
  192.168.32.11   1812  1813  1A7rd


HP ProCurve Switch 5308xl(config)#
```

COMMAND DETAILS

acct-port (p. 284)	host (p. 285)	timeout (p. 286)
auth-port (p. 284)	key (p. 285)	
dead-time (p. 285)	retransmit (p. 286)	

acct-port

- radius-server host *IP-ADDR* acct-port

```
Accounting UDP destination port number (default is 1813).
```

Next Available Option:

- **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 284)**

- radius-server host *IP-ADDR* acct-port *TCP/UDP-PORT*

```
Accounting UDP destination port number (default is 1813).
```

Next Available Options:

- **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 284)**
- **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 285)**

- radius-server host *IP-ADDR* auth-port *TCP/UDP-PORT* acct-port *TCP/UDP-PORT*

```
Accounting UDP destination port number (default is 1813).
```

- radius-server host *IP-ADDR* key *KEY* acct-port *TCP/UDP-PORT*

```
Accounting UDP destination port number (default is 1813).
```

auth-port

- radius-server host *IP-ADDR* acct-port *TCP/UDP-PORT* auth-port *TCP/UDP-PORT*

```
Authentication UDP destination port number (default is 1812).
```

- radius-server host *IP-ADDR* auth-port

```
Authentication UDP destination port number (default is 1812).
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 284)**

■ radius-server host *IP-ADDR* auth-port *TCP/UDP-PORT*

```
Authentication UDP destination port number (default is 1812).
```

Next Available Options:
- **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 284)**
- **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 285)**

■ radius-server host *IP-ADDR* key *KEY* auth-port *TCP/UDP-PORT*

```
Authentication UDP destination port number (default is 1812).
```

dead-time

■ [no] radius-server dead-time

```
Server unavailability  time (default is 0, use the 'no'
form of command to set the dead-time to 0).
```

Supported Values:
- **Min**
- **Max**

Next Available Option:
- **dead-time** < 1 to 1440 > -- Server unavailability time (default is 0, use the 'no' form of command to set the dead-time to 0).**(p. 285)**

■ radius-server dead-time *< 1 to 1440 >*

```
Server unavailability  time (default is 0, use the 'no'
form of command to set the dead-time to 0).
```

Range: < 1 to 1440 >

host

■ [no] radius-server host *IP-ADDR*

```
IP address of the RADIUS server to use.
```

Next Available Options:
- **acct-port** -- Accounting UDP destination port number (default is 1813).**(p. 284)**
- **auth-port** -- Authentication UDP destination port number (default is 1812).**(p. 284)**
- **key** -- Encryption key to use with the RADIUS server (default is NULL).**(p. 285)**

key

■ radius-server host *IP-ADDR* acct-port *TCP/UDP-PORT* key *KEY*

```
Encryption key to use with the RADIUS server (default is NULL).
```

© 2007 Hewlett-Packard Development Company, L.P.

- radius-server host *IP-ADDR* auth-port *TCP/UDP-PORT* key *KEY*

```
Encryption key to use with the RADIUS server (default is NULL).
```

- [no] radius-server host *IP-ADDR* key

```
Encryption key to use with the RADIUS server (default is NULL).
```

Next Available Option:
- **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 285)**

- radius-server host *IP-ADDR* key *KEY*

```
Encryption key to use with the RADIUS server (default is NULL).
```

Next Available Options:
- **auth-port** -- Authentication UDP destination port number (default is 1812). (TCP/UDP-PORT) **(p. 284)**
- **acct-port** -- Accounting UDP destination port number (default is 1813). (TCP/UDP-PORT) **(p. 284)**

- [no] radius-server key

```
Global encryption key (default is NULL).
```

Next Available Option:
- **key** -- Encryption key to use with the RADIUS server (default is NULL). (ASCII-STR) **(p. 285)**

- radius-server key *KEY*

```
Encryption key to use with the RADIUS server (default is NULL).
```

retransmit

- radius-server retransmit *< 1 to 5 >*

```
Number of packet retransmits (default is 3).
```

Range: < 1 to 5 >

timeout

- radius-server timeout *< 1 to 15 >*

```
Server timeout interval (default is 5).
```

Range: < 1 to 15 >

© 2007 Hewlett-Packard Development Company, L.P.

redo

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**repeat (page 291)**

```
Usage: redo [NUMBER|COMMAND-STR]

Description: Re-execute a command from history.
             By default, it executes the last command. If the 'number' is
             specified, it executes the n-th command starting from the most
             recent command in the history. The n is the number specified.
             If the 'COMMAND-STR' is specified, it executes the most recent
             command whose name matches the specified string.
```

COMMAND STRUCTURE

- redo **command** -- The command word identifying a command to execute in the history list. (ASCII-STR) **(p. 287)**
- redo **NUMBER** -- The position of the command to execute in the history list. (NUMBER) **(p. 287)**

COMMAND DETAILS

command (p. 287)	**NUMBER (p. 287)**

command

- redo *COMMAND*

```
The command word identifying a command to execute in the history list.
```

NUMBER

- redo *NUMBER*

```
The position of the command to execute in the history list.
```

© 2007 Hewlett-Packard Development Company, L.P.

reload

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**boot (page 61)**

```
Usage: [no] reload [after  <[[DD:]HH:]MM>  |
                    at  <HH:MM[:SS]>  [<MM/DD[/[YY]YY]>] ]

Description: Warm reboot of the switch. If no parameters are entered,
             an immediate reload is executed.
             [no] - Causes the removal of any pending reboot request.

Parameters:
        o after  - Warm reboot the switch after the given amount of
                   time has passed.
        o at     - Warm reboot the switch at the given time.
```

COMMAND STRUCTURE

- reload **after** -- Warm reboot in a specified amount of time. ([[DD:]HH:]MM) **(p. 288)**
- reload **at** -- Warm reboot at a specified time; If the mm/dd/yy is left blank, the current day is assumed. **(p. 288)**
  - **time** -- Time on given date to do a warm reboot (HH:MM[:SS]) **(p. 289)**
    - **date** -- Date on which a warm reboot is to occur (MM/DD[/[YY]YY]) **(p. 289)**

EXAMPLES

Example: reload

Automatically save your configuration changes and reboot the switch from the same flash image you have been using:

```
HPswitch(config)# max-vlans 12
Command will take effect after saving configuration and reboot.
HPswitch(config)# reload
Device will be rebooted, do you want to continue [y/n]?  y
Do you want to save current configuration [y/n]?  _
```

COMMAND DETAILS

after (p. 288)	**date (p. 289)**
at (p. 288)	**time (p. 289)**

after

- reload after *[[DD:]HH:]MM*

```
Warm reboot in a specified amount of time.
```

at

- reload at

© 2007 Hewlett-Packard Development Company, L.P.

```
Warm reboot at a specified time; If the mm/dd/yy is left blank, the current day is
assumed.
```

Next Available Option:

- **time** -- Time on given date to do a warm reboot (HH:MM[:SS]) **(p. 289)**

date

- reload at *[TIME] [DATE]*

```
Date on which a warm reboot is to occur
```

time

- reload at *[TIME]*

```
Time on given date to do a warm reboot
```

Next Available Option:

- **date** -- Date on which a warm reboot is to occur (MM/DD[/[YY]YY]) **(p. 289)**

© 2007 Hewlett-Packard Development Company, L.P.

rename

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show config (page 341)** **erase (page 136)**

```
Usage: rename config OLDNAME NEWNAME

Description: Change the name of the configuration OLDNAME to NEWNAME.
             No action occurs if there is no configuration named
             OLDNAME, or if a configuration named NEWNAME already
             exists.
```

COMMAND STRUCTURE

- rename **config < config1 >** -- Change the name of the configuration OLDNAME to NEWNAME **(p. 290)**
  - **newname** -- Specify new name for configuration file. (ASCII-STR) **(p. 290)**

COMMAND DETAILS

config (p. 290)	**newname (p. 290)**

config

- rename config *< config 1>*

```
Usage: rename config OLDNAME NEWNAME

Description: Change the name of the configuration OLDNAME to NEWNAME.
             No action occurs if there is no configuration named
             OLDNAME, or if a configuration named NEWNAME already
             exists.
```

Supported Values:
- **config1**

Next Available Option:
- **newname** -- Specify new name for configuration file. (ASCII-STR) **(p. 290)**

newname

- rename config *< config1> NEWNAME*

```
Specify new name for configuration file.
```

© 2007 Hewlett-Packard Development Company, L.P.

repeat

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	redo (page 287)

```
Usage: repeat [NUMBER] [count NUMBER] [delay NUMBER]

Description: Repeat execution of a previous command.
             By default, repeats the last command until a key is pressed.
             If the 'NUMBER' is specified, repeats the n-th most recent
             command where n is the number.
             If the 'count NUMBER' is specified repeat the command
             the NUMBER of times.
             If the 'delay NUMBER' is specified, the iterations are
             separated by the NUMBER of seconds.
```

COMMAND STRUCTURE

- repeat **count** -- Number of repetitions to make. (NUMBER) **(p. 291)**
- repeat **delay** -- Delay between the command executions. (NUMBER) **(p. 291)**
- repeat **NUMBER** -- Specify the position of the command to execute in the history list. (NUMBER) **(p. 291)**

COMMAND DETAILS

count (p. 291)	**delay (p. 291)**	**NUMBER (p. 291)**

count

- repeat count *NUMBER*

```
Number of repetitions to make.
```

delay

- repeat delay *NUMBER*

```
Delay between the command executions.
```

NUMBER

- repeat *NUMBER*

```
Specify the position of the command to execute in the history list.
```

© 2007 Hewlett-Packard Development Company, L.P.

router

OVERVIEW

Category:	Routing
Primary context:	config
Related Commands	**ip (page 180)** **vlan (page 457)** **show ip (page 358)**

```
Usage: [no] router ...

Description: Configure the switch routing protocols. You can enter the commands from
             the global configuration context or the RIP, OSPF, or PIM configuration
             contexts. For example, to enter an OSPF command from the global
             configuration context, use the "router" keyword in front of the command.
             To enter an OSPF command in the OSPF configuration context, type
             "router ospf" to change to the OSPF configuration context, then type
             the command without the "router" keyword.

             Use 'router ?' to see a list of all possible options.
```

NOTES

Enabling IP Routing First

To access the RIP, OSPF, or PIM configuration context, you must enable IP routing first.

COMMAND STRUCTURE

- [no] router **ospf** -- Enable/disable/configure Open Shortest Path First (OSPF) protocol on the device, or enter OSPF Configuration Context **(p. 304)**
  - **area** -- Define/remove an OSPF area, area range or virtual link **(p. 295)**
    - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 296)**
      - **normal** -- Define a "normal" area. **(p. 303)**
      - **nssa < 0 to 16777215 >** -- Define a "not-so-stubby" area (or NSSA) and its cost. **(p. 303)**
        - **metric-type < type1 | type2 >** -- Metric type of the type-7 default. **(p. 302)**
        - **no-summary** -- Do not send summary LSA into the area. **(p. 303)**
      - **range** -- Summarize routes matching address/mask pair. **(p. 305)**
        - **ip** -- Specify IP address/mask pair. (IP-ADDR/MASK-LENGTH) **(p. 301)**
        - **no-advertise** -- Do not advertise the range outside the area. **(p. 302)**
        - **type < summary | nssa >** -- Link state database type to apply the range. **(p. 312)**
      - **stub** -- Define a "stub" area and specify its cost. **(p. 309)**
        - **cost < 0 to 16777215 >** -- Enter cost to use when injecting default routes into the area. **(p. 298)**
        - **no-summary** -- Do not send summary LSA into the area. **(p. 303)**
      - **virtual-link** -- Specify a virtual neighbor. (IP-ADDR) **(p. 312)**
        - **authentication** -- Disable authentication. **(p. 296)**
        - **authentication-key** -- Set simple authentication method and key. **(p. 296)**
          - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 296)**
        - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 299)**
        - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 300)**

© 2007 Hewlett-Packard Development Company, L.P.

- **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 302)**
  - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 298)**
- **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 306)**
- **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 309)**

- **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 297)**
  - **normal** -- Define a "normal" area. **(p. 303)**
  - **nssa < 0 to 16777215 >** -- Define a "not-so-stubby" area (or NSSA) and its cost. **(p. 303)**
    - **metric-type < type1 | type2 >** -- Metric type of the type-7 default. **(p. 302)**
    - **no-summary** -- Do not send summary LSA into the area. **(p. 303)**
  - **range** -- Summarize routes matching address/mask pair. **(p. 305)**
    - **ip** -- Specify IP address/mask pair. (IP-ADDR/MASK-LENGTH) **(p. 301)**
    - **no-advertise** -- Do not advertise the range outside the area. **(p. 302)**
    - **type < summary | nssa >** -- Link state database type to apply the range. **(p. 312)**
  - **stub** -- Define a "stub" area and specify its cost. **(p. 309)**
    - **cost < 0 to 16777215 >** -- Enter cost to use when injecting default routes into the area. **(p. 298)**
    - **no-summary** -- Do not send summary LSA into the area. **(p. 303)**
  - **virtual-link** -- Specify a virtual neighbor. (IP-ADDR) **(p. 312)**
    - **authentication** -- Disable authentication. **(p. 296)**
    - **authentication-key** -- Set simple authentication method and key. **(p. 296)**
      - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 296)**
    - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 299)**
    - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 300)**
    - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 302)**
      - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 298)**
    - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 306)**
    - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 309)**

- **default-metric < 0 to 16777215 >** -- The default metric used for advertising external routes imported into OSPF by this router **(p. 299)**
- **distance** -- Set administrative distance to associate with intra-area, inter-area and AS-external routes learned by OSPF **(p. 299)**
  - **external < 1 to 255 >** -- Set administrative distance to associate with external routes learned by OSPF. **(p. 300)**
  - **inter-area < 1 to 255 >** -- Set administrative distance to associate with inter-area routes learned by OSPF. **(p. 301)**
  - **intra-area < 1 to 255 >** -- Set administrative distance to associate with intra-area routes learned by OSPF. **(p. 301)**
- **metric-type < type1 | type2 >** -- The default metric type used for advertising external routes imported into OSPF by this router **(p. 302)**
- **redistribute < connected | static | rip >** -- Specify source protocols which will be redistributed into OSPF **(p. 305)**
- **restrict** -- Prevent redistribution of routes via OSPF **(p. 306)**
  - **ip-addr** -- Prevent redistribution of routes via OSPF (IP-ADDR/MASK-LENGTH) **(p. 301)**
- **rfc1583-compatibility** -- Enable/disable RFC-1583 compatibility **(p. 306)**
- **trap < virtual-interface-state-change | neighbor-state-change | virtual-neighbor-state-change | ... >** -- Enable/disable OSPF traps **(p. 310)**

■ [no] router **pim** -- Enable/disable/configure PIM protocol on the device, or enter PIM Configuration Context **(p. 304)**

© 2007 Hewlett-Packard Development Company, L.P.

- **bsr-candidate** -- Configure the router to advertise itself as the Candidate Bootstrap Router (Candidate-BSR) for a PIM-SM domain **(p. 297)**
  - **bsm-interval < 5 to 300 >** -- Specify the interval for sending Bootstrap messages on PIM-SM interfaces. **(p. 297)**
  - **hash-mask-length < 1 to 32 >** -- Specify the length (in bits) of the hash mask. **(p. 300)**
  - **priority < 0 to 255 >** -- Specify the priority for the Candidate Bootstrap router. **(p. 305)**
  - **source-ip-vlan** -- Specify the VLAN to use as a source for Candidate-BSR router IP address (PIM-SM must be enabled on this VLAN). (VLAN-ID) **(p. 309)**
- **join-prune-interval < 5 to 65535 >** -- Configure interval at which the router will send periodic PIM-SM Join/Prune messages **(p. 302)**
- **rp-address** -- Statically configure the Rendezvous Point (RP) to accept multicast traffic for specified group or range of groups **(p. 307)**
  - **IP-ADDR** -- Specify the IP address of the static RP. (IP-ADDR) **(p. 301)**
    - **GROUP-ADDR/GROUP-MASK** -- Specify the range of multicast group addresses associated with the static RP. (IP-ADDR/MASK-LENGTH) **(p. 300)**
      - **override** -- Specify whether or not static RP configuration precedes the information learned by a BSR. **(p. 304)**
- **rp-candidate** -- Configure router to advertise itself as the Candidate Rendezvous Point (Candidate-RP) to the Bootstrap Router (BSR) **(p. 308)**
  - **group-prefix** -- Specify the multicast group prefix to associate with the Candidate-RP router. **(p. 300)**
    - **GROUP-ADDR/GROUP-MASK** -- Enter the address and mask to define the multicast group range. (IP-ADDR/MASK-LENGTH) **(p. 300)**
  - **hold-time < 30 to 255 >** -- Specify the hold time value to be send in C-RP-Adv messages. **(p. 301)**
  - **priority < 0 to 255 >** -- Specify the priority for the Candidate-RP router. **(p. 305)**
  - **source-ip-vlan** -- Specify the VLAN to use as a source for Candidate-RP router IP address (PIM-SM must be enabled on this VLAN). (VLAN-ID) **(p. 309)**
    - **group-prefix** -- Specify the multicast group prefix to associate with the Candidate-RP router. **(p. 300)**
      - **GROUP-ADDR/GROUP-MASK** -- Enter the address and mask to define the multicast group range. (IP-ADDR/MASK-LENGTH) **(p. 300)**
- **spt-threshold** -- Specify whether switching to the Shortest Path Tree is enabled or disabled on the router **(p. 309)**
- **state-refresh < 10 to 300 >** -- Set the interval between successive State Refresh messages originated by this router **(p. 309)**
- **trap < neighbor-loss | hardware-mrt-full | software-mrt-full | ... >** -- Enable/disable PIM traps **(p. 310)**

■ [no] router **rip** -- Enable/disable/configure Routing Internet Protocol (RIP) on the device, or enter RIP Configuration Context **(p. 307)**
- **auto-summary** -- Enable/disable advertisement of summarized routes **(p. 297)**
- **default-metric < 1 to 15 >** -- Set default metric for imported routes **(p. 299)**
- **distance < 1 to 255 >** -- Set administrative distance for routes learned via RIP **(p. 299)**
- **redistribute < connected | static | ospf >** -- Specify source protocols which will be redistributed into RIP **(p. 305)**
- **restrict** -- Prevent redistribution of routes via RIP **(p. 306)**
  - **ip-addr** -- Prevent redistribution of routes via RIP (IP-ADDR/MASK-LENGTH) **(p. 301)**

■ [no] router **vrrp** -- Enable/disable/configure Virtual Router Redundancy Protocol (VRRP) on the device **(p. 313)**
- **traps** -- Enable/disable generation of VRRP traps **(p. 311)**

© 2007 Hewlett-Packard Development Company, L.P.

COMMAND DETAILS

area (p. 295)
area-id (p. 296)
authentication (p. 296)
authentication-key (p. 296)
auto-summary (p. 297)
backbone (p. 297)
bsm-interval (p. 297)
bsr-candidate (p. 297)
chain-name (p. 298)
cost (p. 298)
dead-interval (p. 299)
default-metric (p. 299)
distance (p. 299)
external (p. 300)
GROUP-ADDR/GROUP-MASK (p. 300)
group-prefix (p. 300)
hash-mask-length (p. 300)
hello-interval (p. 300)
hold-time (p. 301)
inter-area (p. 301)
intra-area (p. 301)
ip (p. 301)
ip-addr (p. 301)
IP-ADDR (p. 301)
join-prune-interval (p. 302)
md5-auth-key-chain (p. 302)
metric-type (p. 302)
no-advertise (p. 302)
normal (p. 303)
no-summary (p. 303)
nssa (p. 303)
ospf (p. 304)
override (p. 304)
pim (p. 304)
priority (p. 305)
range (p. 305)
redistribute (p. 305)
restrict (p. 306)
retransmit-interval (p. 306)
rfc1583-compatibility (p. 306)
rip (p. 307)
rp-address (p. 307)
rp-candidate (p. 308)
source-ip-vlan (p. 309)
spt-threshold (p. 309)
state-refresh (p. 309)
stub (p. 309)
transit-delay (p. 309)
trap (p. 310)
traps (p. 311)
type (p. 312)
virtual-link (p. 312)
vrrp (p. 313)

area

- [no] router ospf area

```
Usage:    area <OSPF-AREA-ID|backbone> [normal]
          area <OSPF-AREA-ID|backbone> stub <0-16777215> [no-summary]
          area <OSPF-AREA-ID|backbone> range IP-ADDR/MASK-LENGTH
                                       [no-advertise]
          area <OSPF-AREA-ID|backbone> virtual-link IP-ADDR
                                       [transit-delay <0-3600>]
                                       [retransmit-interval <0-3600>]
                                       [hello-interval <1-65535>]
                                       [dead-interval <0-2147483647>]
          area <OSPF-AREA-ID|backbone> virtual-link IP-ADDR
                                       authentication-key OCTET-STR
          area <OSPF-AREA-ID|backbone> virtual-link IP-ADDR
                                       md5-auth-key-chain CHAIN-NAME-STR
       no area <OSPF-AREA-ID|backbone>
       no area <OSPF-AREA-ID|backbone> range IP-ADDR/MASK-LENGTH
       no area <OSPF-AREA-ID|backbone> virtual-link IP-ADDR
                                       [authentication]

Description: Define/remove an OSPF area, area range or virtual link.
           - 'area... [normal]' command defines a normal area. Area can be
             identified by a single integer or an IP address style dotted
             decimal. Use 0.0.0.0 address or 'backbone' keyword to specify the
             backbone area.
           - 'area... stub...' defines a "stub" area and cost to use when
             injecting default routes of a border router into the area. If
             'no-summary' is specified then no summary LSA will be sent into
             the area.
           - 'area... range...' defines a range of IP addresses the area
             consists of and directs to summarize routes matching the range.
             If 'no-advertise' is specified then the range will not be
             advertised outside the area.
           - 'area... virtual-link...' defines a virtual link along with its
```

© 2007 Hewlett-Packard Development Company, L.P.

```
time duration parameters:
'transit-delay' - The estimated number of seconds it takes to
transmit a link state update packet over the link.
'retransmit-interval' - The number of seconds between link-state
advertisement retransmissions. This value is also used when
retransmitting database description and link-state request packets.
'hello-interval' - The number of seconds between the Hello packets
those the router sends to the virtual neighbor.
'dead-interval' - The number of seconds that a router's Hello
packets have not been seen before it's neighbor declares the
router down. This should be some multiple of the Hello interval.
- 'area... virtual-link... authentication-key...' - specifies the
authentication key to be used to maintain the virtual link. Note
that unauthenticated link need no authentication key, and simple
password authentication cannot use a key of more than 8 octets.
- 'area... virtual-link... md5-auth-key-chain...' -
specifies the key chain to pick keys for MD5 authentication
from and configures the virtual link to MD5 authentication.
- 'no area...' removes the entire area.
- 'no area... range...' removes the specified range.
- 'no area... virtual-link...' removes the specified virtual link,
and 'no area... virtual-link... authentication' unsets the
authentication on the link.
```

Next Available Options:

- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 296)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 297)**

area-id

- router ospf area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

Next Available Options:

- **normal** -- Define a "normal" area.**(p. 303)**
- **nssa** < 0 to 16777215 > -- Define a "not-so-stubby" area (or NSSA) and its cost.**(p. 303)**
- **stub** -- Define a "stub" area and specify its cost.**(p. 309)**
- **range** -- Summarize routes matching address/mask pair.**(p. 305)**
- **virtual-link** -- Specify a virtual neighbor. (IP-ADDR) **(p. 312)**

authentication

- [no] router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* authentication

```
Disable authentication.
```

- [no] router ospf area backbone virtual-link *IP-ADDR* authentication

```
Disable authentication.
```

authentication-key

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* authentication-key

```
Set simple authentication method and key.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 296)**

■ router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

■ router ospf area backbone virtual-link *IP-ADDR* authentication-key

```
Set simple authentication method and key.
```

Next Available Option:
- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 296)**

■ router ospf area backbone virtual-link *IP-ADDR* authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

auto-summary

■ [no] router rip auto-summary

```
Usage: [no] auto-summary

Description: Enable/disable advertisement of summarized routes.
             Summarization mechanisms should be disabled when using both
             version 1 and version 2 of RIP within a single network.
```

backbone

■ router ospf area backbone

```
The backbone area (the same as 0.0.0.0).
```

Next Available Options:
- **normal** -- Define a "normal" area.**(p. 303)**
- **nssa** < 0 to 16777215 > -- Define a "not-so-stubby" area (or NSSA) and its cost.**(p. 303)**
- **stub** -- Define a "stub" area and specify its cost.**(p. 309)**
- **range** -- Summarize routes matching address/mask pair.**(p. 305)**
- **virtual-link** -- Specify a virtual neighbor. (IP-ADDR) **(p. 312)**

bsm-interval

■ router pim bsr-candidate bsm-interval *< 5 to 300 >*

```
Specify the interval for sending Bootstrap messages on PIM-SM interfaces.
```

Range: < 5 to 300 >

bsr-candidate

■ [no] router pim bsr-candidate

```
Usage: bsr-candidate [source-ip-vlan <VLAN-ID>]
                     [hash-mask-length <1-32>]
                     [priority <0-255>]
                     [bsm-interval <5-300>]
```

© 2007 Hewlett-Packard Development Company, L.P.

```
    no bsr-candidate [source-ip-vlan <VLAN-ID>]

Description: Configure the router to advertise itself as the Candidate
             Bootstrap Router (Candidate-BSR) for a PIM-SM domain. When
             enabling router to be a Candidate-BSR the VLAN ID must be
             specified, which IP address will be advertised as a
             Candidate-BSR address. PIM-SM must be enabled on the VLAN.
             Use 'no' form of this command to disable the router to be a
             Candidate-BSR.
             NOTE: It is recommended that the same routing switch is
                   configured as both the Candidate-BSR and the Candidate-RP.
Parameters:

    o source-ip-vlan <VLAN-ID> - The VLAN which IP address will be advertised
             as the Candidate-BSR IP address.
    o hash-mask-length <1-32> - The mask length (in bits) used by the
             PIM-SM hash function when selecting an RP. The default is 30.
    o priority <0-255> - The priority for the Candidate-BSR for the
             local PIM-SM domain. The larger value means the higher priority.
             The default is 0.
    o bsm-interval <5-300> - The interval (in seconds) for sending periodic
             Bootstrap messages on all PIM-SM interfaces, when this router is
             the elected BSR. The default is 60 seconds.
```

Next Available Options:

- **source-ip-vlan** -- Specify the VLAN to use as a source for Candidate-BSR router IP address (PIM-SM must be enabled on this VLAN). (VLAN-ID) **(p. 309)**
- **hash-mask-length** < 1 to 32 > -- Specify the length (in bits) of the hash mask. **(p. 300)**
- **priority** < 0 to 255 > -- Specify the priority for the Candidate Bootstrap router. **(p. 305)**
- **bsm-interval** < 5 to 300 > -- Specify the interval for sending Bootstrap messages on PIM-SM interfaces. **(p. 297)**

chain-name

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

- router ospf area backbone virtual-link *IP-ADDR* md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

cost

- router ospf area *OSPF-AREA-ID* stub *< 0 to 16777215 >*

```
Enter cost to use when injecting default routes
into the area.
```

Range: < 0 to 16777215 >

- router ospf area backbone stub *< 0 to 16777215 >*

```
Enter cost to use when injecting default routes
into the area.
```

Range: < 0 to 16777215 >

© 2007 Hewlett-Packard Development Company, L.P.

dead-interval

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* dead-interval *< 1 to 65535 >*

```
Set dead interval in seconds; the default is 40.
```

Range: < 1 to 65535 >

- router ospf area backbone virtual-link *IP-ADDR* dead-interval *< 1 to 65535 >*

```
Set dead interval in seconds; the default is 40.
```

Range: < 1 to 65535 >

default-metric

- router ospf default-metric *< 0 to 16777215 >*

```
Usage: default-metric <0-16777215>

Description: The default metric used for advertising external routes imported
             into OSPF by this router.
```

Range: < 0 to 16777215 >

- router rip default-metric *< 1 to 15 >*

```
Usage: default-metric <1-15>

Description: Set default metric for imported routes.
             Default value is 1.
```

Range: < 1 to 15 >

distance

- router ospf distance

```
Usage: distance <intra-area|inter-area|external> <1-255>

Description: Set administrative distance to associate with intra-area,
             inter-area and AS-external routes learned by OSPF. Default
             value is 110 for all types of OSPF routes.
```

Next Available Options:

- **intra-area** < 1 to 255 > -- Set administrative distance to associate with intra-area routes learned by OSPF.**(p. 301)**
- **inter-area** < 1 to 255 > -- Set administrative distance to associate with inter-area routes learned by OSPF.**(p. 301)**
- **external** < 1 to 255 > -- Set administrative distance to associate with external routes learned by OSPF.**(p. 300)**

- router rip distance *< 1 to 255 >*

```
Usage: distance <1-255>

Description: Set administrative distance for routes learned via RIP.
             Default value is 120.
```

Range: < 1 to 255 >

© 2007 Hewlett-Packard Development Company, L.P.

external

- [no] router ospf distance external *< 1 to 255 >*

  `Set administrative distance to associate with external routes learned by OSPF.`

  Range: < 1 to 255 >

GROUP-ADDR/GROUP-MASK

- [no] router pim rp-address *IP-ADDR IP-ADDR/MASK-LENGTH*

  `Specify the range of multicast group addresses associated with the static RP.`

  Next Available Option:
  - **override** -- Specify whether or not static RP configuration precedes the information learned by a BSR. **(p. 304)**

- router pim rp-candidate source-ip-vlan *VLAN-ID* group-prefix *IP-ADDR/MASK-LENGTH*

  `Enter the address and mask to define the multicast group range.`

- router pim rp-candidate group-prefix *IP-ADDR/MASK-LENGTH*

  `Enter the address and mask to define the multicast group range.`

group-prefix

- router pim rp-candidate source-ip-vlan *VLAN-ID* group-prefix

  `Specify the multicast group prefix to associate with the Candidate-RP router.`

  Next Available Option:
  - **GROUP-ADDR/GROUP-MASK** -- Enter the address and mask to define the multicast group range. (IP-ADDR/MASK-LENGTH) **(p. 300)**

- [no] router pim rp-candidate group-prefix

  `Specify the multicast group prefix to associate with the Candidate-RP router.`

  Next Available Option:
  - **GROUP-ADDR/GROUP-MASK** -- Enter the address and mask to define the multicast group range. (IP-ADDR/MASK-LENGTH) **(p. 300)**

hash-mask-length

- router pim bsr-candidate hash-mask-length *< 1 to 32 >*

  `Specify the length (in bits) of the hash mask.`

  Range: < 1 to 32 >

hello-interval

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* hello-interval *< 1 to 65535 >*

  `Set hello interval in seconds; the default is 10.`

  Range: < 1 to 65535 >

© 2007 Hewlett-Packard Development Company, L.P.

- router ospf area backbone virtual-link *IP-ADDR* hello-interval *< 1 to 65535 >*

  Set hello interval in seconds; the default is 10.

  Range: < 1 to 65535 >

hold-time

- router pim rp-candidate hold-time *< 30 to 255 >*

  Specify the hold time value to be send in C-RP-Adv messages.

  Range: < 30 to 255 >

inter-area

- [no] router ospf distance inter-area *< 1 to 255 >*

  Set administrative distance to associate with inter-area routes learned by OSPF.

  Range: < 1 to 255 >

intra-area

- [no] router ospf distance intra-area *< 1 to 255 >*

  Set administrative distance to associate with intra-area routes learned by OSPF.

  Range: < 1 to 255 >

ip

- router ospf area *OSPF-AREA-ID* range *IP-ADDR/MASK-LENGTH*

  Specify IP address/mask pair.

- router ospf area backbone range *IP-ADDR/MASK-LENGTH*

  Specify IP address/mask pair.

ip-addr

- [no] router ospf restrict *IP-ADDR/MASK-LENGTH*

  Usage: [no] restrict IP-ADDR/MASK-LEN

  Description: Prevent redistribution of routes via OSPF.

- [no] router rip restrict *IP-ADDR/MASK-LENGTH*

  Usage: [no] restrict IP-ADDR/MASK-LEN

  Description: Prevent redistribution of routes via RIP.

IP-ADDR

- [no] router pim rp-address *IP-ADDR*

  Specify the IP address of the static RP.

  Next Available Option:
  - **GROUP-ADDR/GROUP-MASK** -- Specify the range of multicast group addresses associated with the static RP. (IP-ADDR/MASK-LENGTH) **(p. 300)**

© 2007 Hewlett-Packard Development Company, L.P.

join-prune-interval

- router pim join-prune-interval *< 5 to 65535 >*

```
Usage: join-prune-interval <1-65535>

Description: Configure interval at which the router will send periodic
             PIM-SM Join/Prune messages. Default is 60 seconds.
```

Range: < 5 to 65535 >

md5-auth-key-chain

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* md5-auth-key-chain

```
Set MD5 authentication method and key chain.
```

Next Available Option:

- **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 298)**

- router ospf area backbone virtual-link *IP-ADDR* md5-auth-key-chain

```
Set MD5 authentication method and key chain.
```

Next Available Option:

- **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 298)**

metric-type

- router ospf area *OSPF-AREA-ID* nssa *< 0 to 16777215 >* metric-type *< type1 | type2 >*

```
Metric type of the type-7 default.
```

Supported Values:

- **type1** -- Comparable (an OSPF metric plus the external metric).
- **type2** -- Non-comparable metric (the external metric).

- router ospf area backbone nssa *< 0 to 16777215 >* metric-type *< type1 | type2 >*

```
Metric type of the type-7 default.
```

Supported Values:

- **type1** -- Comparable (an OSPF metric plus the external metric).
- **type2** -- Non-comparable metric (the external metric).

- router ospf metric-type *< type1 | type2 >*

```
Usage: metric-type <type1|type2>

Description: The default metric type used for advertising external routes
             imported into OSPF by this router.
```

Supported Values:

- **type1** -- Comparable (an OSPF metric plus the external metric).
- **type2** -- Non-comparable metric (the external metric).

no-advertise

- router ospf area *OSPF-AREA-ID* range no-advertise

© 2007 Hewlett-Packard Development Company, L.P.

```
Do not advertise the range outside the area.
```

- router ospf area backbone range no-advertise

```
Do not advertise the range outside the area.
```

normal

- router ospf area *OSPF-AREA-ID* normal

```
Define a "normal" area.
```

- router ospf area backbone normal

```
Define a "normal" area.
```

no-summary

- router ospf area *OSPF-AREA-ID* nssa *< 0 to 16777215 >* no-summary

```
Do not send summary LSA into the area.
```

- router ospf area *OSPF-AREA-ID* stub no-summary

```
Do not send summary LSA into the area.
```

- router ospf area backbone nssa *< 0 to 16777215 >* no-summary

```
Do not send summary LSA into the area.
```

- router ospf area backbone stub no-summary

```
Do not send summary LSA into the area.
```

nssa

- router ospf area *OSPF-AREA-ID* nssa *< 0 to 16777215 >*

```
Define a "not-so-stubby" area (or NSSA) and its cost.
```

Range: < 0 to 16777215 >

Next Available Options:
- **metric-type** < type1 | type2 > -- Metric type of the type-7 default.**(p. 302)**
- **no-summary** -- Do not send summary LSA into the area.**(p. 303)**

- router ospf area backbone nssa *< 0 to 16777215 >*

```
Define a "not-so-stubby" area (or NSSA) and its cost.
```

Range: < 0 to 16777215 >

Next Available Options:
- **metric-type** < type1 | type2 > -- Metric type of the type-7 default.**(p. 302)**
- **no-summary** -- Do not send summary LSA into the area.**(p. 303)**

© 2007 Hewlett-Packard Development Company, L.P.

ospf

- [no] router ospf

```
Usage: [no] router ospf [...]

Description: Enable/disable/configure Open Shortest Path First (OSPF)
             protocol on the device, or enter OSPF Configuration Context.
             Called without 'no', the command enables OSPF on the device
             and changes current context to OSPF Configuration Context.
             Otherwise ('no' is specified) the command disables OSPF. The
             command can be followed by an OSPF configuration command. Use
             'router ospf ?' to get a list of all possible options.
```

Next Available Options:

- **area** -- Define/remove an OSPF area, area range or virtual link**(p. 295)**
- **default-metric** < 0 to 16777215 > -- The default metric used for advertising external routes imported into OSPF by this router**(p. 299)**
- **distance** -- Set administrative distance to associate with intra-area, inter-area and AS-external routes learned by OSPF**(p. 299)**
- **metric-type** < type1 | type2 > -- The default metric type used for advertising external routes imported into OSPF by this router**(p. 302)**
- **redistribute** < connected | static | rip > -- Specify source protocols which will be redistributed into OSPF**(p. 305)**
- **restrict** -- Prevent redistribution of routes via OSPF**(p. 306)**
- **rfc1583-compatibility** -- Enable/disable RFC-1583 compatibility**(p. 306)**
- **trap** < virtual-interface-state-change | neighbor-state-change | virtual-neighbor-state-change | ... > -- Enable/disable OSPF traps**(p. 310)**

override

- [no] router pim rp-address *IP-ADDR IP-ADDR/MASK-LENGTH* override

```
Specify whether or not static RP configuration precedes the information
learned by a BSR.
```

pim

- [no] router pim

```
Usage: [no] router pim [...]

Description: Enable/disable/configure PIM protocol on the device, or enter
             PIM Configuration Context.
             Called without 'no', the command enables PIM on the device
             and changes current context to PIM Configuration Context.
             Otherwise, the command disables PIM. The command can be
             followed by a PIM configuration command. Use 'router pim ?' to
             get a list of all possible options.
```

Next Available Options:

- **bsr-candidate** -- Configure the router to advertise itself as the Candidate Bootstrap Router (Candidate-BSR) for a PIM-SM domain**(p. 297)**
- **rp-address** -- Statically configure the Rendezvous Point (RP) to accept multicast traffic for specified group or range of groups**(p. 307)**
- **rp-candidate** -- Configure router to advertise itself as the Candidate Rendezvous Point (Candidate-RP) to the Bootstrap Router (BSR)**(p. 308)**

© 2007 Hewlett-Packard Development Company, L.P.

- **join-prune-interval** < 5 to 65535 > -- Configure interval at which the router will send periodic PIM-SM Join/Prune messages**(p. 302)**
- **spt-threshold** -- Specify whether switching to the Shortest Path Tree is enabled or disabled on the router**(p. 309)**
- **state-refresh** < 10 to 300 > -- Set the interval between successive State Refresh messages originated by this router**(p. 309)**
- **trap** < neighbor-loss | hardware-mrt-full | software-mrt-full | ... > -- Enable/disable PIM traps**(p. 310)**

priority

- router pim bsr-candidate priority *< 0 to 255 >*

```
Specify the priority for the Candidate Bootstrap router.
```

Range: < 0 to 255 >

- router pim rp-candidate priority *< 0 to 255 >*

```
Specify the priority for the Candidate-RP router.
```

Range: < 0 to 255 >

range

- [no] router ospf area *OSPF-AREA-ID* range

```
Summarize routes matching address/mask pair.
```

Next Available Options:
- **ip** -- Specify IP address/mask pair. (IP-ADDR/MASK-LENGTH) **(p. 301)**
- **no-advertise** -- Do not advertise the range outside the area.**(p. 302)**
- **type** < summary | nssa > -- Link state database type to apply the range.**(p. 312)**

- [no] router ospf area backbone range

```
Summarize routes matching address/mask pair.
```

Next Available Options:
- **ip** -- Specify IP address/mask pair. (IP-ADDR/MASK-LENGTH) **(p. 301)**
- **no-advertise** -- Do not advertise the range outside the area.**(p. 302)**
- **type** < summary | nssa > -- Link state database type to apply the range.**(p. 312)**

redistribute

- [no] router ospf redistribute *< connected | static | rip >*

```
Usage: [no] redistribute <static|connected|rip>

Description: Specify source protocols which will be redistributed
             into OSPF.  Use the [no] form of the command to disable
             redistribution of the specified protocol.

    o static    -- redistribute from manually configured routes.
    o connected -- redistribute from locally connected network(s).
    o rip       -- redistribute from RIP routes.
```

© 2007 Hewlett-Packard Development Company, L.P.

Supported Values:
- **connected**
- **static**
- **rip**

■ [no] router rip redistribute *< connected | static | ospf >*

```
Usage: [no] redistribute <static|connected|ospf>

Description: Specify source protocols which will be redistributed
             into RIP.  Use the [no] form of the command to disable
             redistribution of the specified protocol.

    o static    -- redistribute manually configured routes.
    o connected -- redistribute locally connected network(s).
    o ospf      -- redistribute OSPF routes.
```

Supported Values:
- **connected**
- **static**
- **ospf**

restrict

■ router ospf restrict

```
Usage: [no] restrict IP-ADDR/MASK-LEN

Description: Prevent redistribution of routes via OSPF.
```

Next Available Option:
- **ip-addr** -- Prevent redistribution of routes via OSPF (IP-ADDR/MASK-LENGTH) **(p. 301)**

■ router rip restrict

```
Usage: [no] restrict IP-ADDR/MASK-LEN

Description: Prevent redistribution of routes via RIP.
```

Next Available Option:
- **ip-addr** -- Prevent redistribution of routes via RIP (IP-ADDR/MASK-LENGTH) **(p. 301)**

retransmit-interval

■ router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

■ router ospf area backbone virtual-link *IP-ADDR* retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

rfc1583-compatibility

■ [no] router ospf rfc1583-compatibility

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] rfc-1583-compatibility

Description: Enable/disable RFC-1583 compatibility. This controls the
             preference rules used when choosing among multiple
             AS-external-LSAs advertising the same destination. When RFC-1583
             compatibility is disabled, the preference rules are those stated
             in RFC-2328, which prevent routing loops when AS-external-LSAs
             for the same destination have been originated from different
             areas. In order to minimize the chance of routing loops, all OSPF
             routers in an OSPF routing domain should have this parameter to
             be identical. When there are routers present that have not been
             updated with the functionality specified in RFC-2328, all routers
             should have RFC-1583 compatibility enabled. Otherwise, all routers
             should have RFC-1583 compatibility disabled, preventing routing
             loops.
```

rip

- [no] router rip

```
Usage: [no] router rip [...]

Description: Enable/disable/configure Routing Internet Protocol (RIP)
             on the device, or enter RIP Configuration Context.
             Called without 'no', the command enables RIP on the device
             and changes current context to RIP Configuration Context.
             Otherwise, the command disables RIP. The command can be
             followed by a RIP configuration command. Use 'router rip ?' to
             get a list of all possible options.
```

Next Available Options:

- **auto-summary** -- Enable/disable advertisement of summarized routes**(p. 297)**
- **default-metric** < 1 to 15 > -- Set default metric for imported routes**(p. 299)**
- **distance** < 1 to 255 > -- Set administrative distance for routes learned via RIP**(p. 299)**
- **redistribute** < connected | static | ospf > -- Specify source protocols which will be redistributed into RIP**(p. 305)**
- **restrict** -- Prevent redistribution of routes via RIP**(p. 306)**

rp-address

- [no] router pim rp-address

```
Usage: [no] rp-address <IP-ADDR> [GROUP-ADDR/GROUP-MASK] [override]

Description: Statically configure the Rendezvous Point (RP) to accept
             multicast traffic for specified group or range of groups.
             If GROUP-ADDR/GROUP-MASK is not specified, the default multicast
             group prefix 224.0.0.0/4 (224.0.0.0 240.0.0.0) will be used.
             To remove all entries associated with the RP or a specific
             entry use 'no' form of the command.

Parameters:

    o IP-ADDR    - IP address of the Rendezvous Point.
    o GROUP-ADDR - IP address of multicast group, when combined
                   with GROUP-MASK, gives the group prefix.
    o GROUP-MASK - Defines the range of multicast group addresses.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
    o override    - Sets the precedence of statically configured RP higher
                    than dynamically learned RPs. Not set by default.
```

Next Available Option:

- **IP-ADDR** -- Specify the IP address of the static RP. (IP-ADDR) **(p. 301)**

rp-candidate

- [no] router pim rp-candidate

```
Usage: rp-candidate [source-ip-vlan <VLAN-ID>]
                    [group-prefix <GROUP-ADDR/GROUP-MASK>]
                    [hold-time <30-255>]
                    [priority <0-255>]
    no rp-candidate [source-ip-vlan <VLAN-ID>]
                    [group-prefix <GROUP-ADDR/GROUP-MASK>]

Description: Configure router to advertise itself as the Candidate
             Rendezvous Point (Candidate-RP) to the Bootstrap Router (BSR).
             When enabling router to be a Candidate-RP the VLAN ID must
             be specified, which IP address will be advertised as a
             Candidate-RP's IP address. PIM-SM must be enabled on the VLAN.
             If GROUP-ADDR/GROUP-MASK is not specified the router will be a
             Candidate-RP for all multicast groups. Use 'no' form of this
             command to remove specific multicast group or disable the router
             to be a Candidate-RP.
             NOTE: It is recommended that the same routing switch is configured
                   as the Candidate-BSR and the Candidate-RP.
Parameters:

    o source-ip-vlan <VLAN-ID> - The VLAN which IP address will be advertised
             as the Candidate-RP address.
    o group-prefix <GROUP-ADDR/GROUP-MASK> - The address and mask that specify
             the multicast group(s) the router uses to advertise in association
             with the Candidate-RP address.
    o hold-time <3-255> - The hold time value (in seconds) to be send to the
             BSR in C-RP-Adv messages. This tells the BSR for how long it
             should consider the sending Candidate-RP router to be operative.
             The default is 150 seconds.
             Note: This value is set to '0' when local system is not a
                   Candidate-RP.
    o priority <0-255> - The priority for the Candidate-RP router for the
             local PIM-SM domain. The smaller value means the higher priority.
             The default is 192.
```

Next Available Options:

- **hold-time** < 30 to 255 > -- Specify the hold time value to be send in C-RP-Adv messages. **(p. 301)**
- **priority** < 0 to 255 > -- Specify the priority for the Candidate-RP router. **(p. 305)**
- **source-ip-vlan** -- Specify the VLAN to use as a source for Candidate-RP router IP address (PIM-SM must be enabled on this VLAN). (VLAN-ID) **(p. 309)**
- **group-prefix** -- Specify the multicast group prefix to associate with the Candidate-RP router. **(p. 300)**

© 2007 Hewlett-Packard Development Company, L.P.

source-ip-vlan

- [no] router pim bsr-candidate source-ip-vlan *VLAN-ID*

```
Specify the VLAN to use as a source for Candidate-BSR router IP address
(PIM-SM must be enabled on this VLAN).
```

- [no] router pim rp-candidate source-ip-vlan *VLAN-ID*

```
Specify the VLAN to use as a source for Candidate-RP router IP address
(PIM-SM must be enabled on this VLAN).
```

Next Available Option:

- **group-prefix** -- Specify the multicast group prefix to associate with the Candidate-RP router. **(p. 300)**

spt-threshold

- [no] router pim spt-threshold

```
Usage: [no] spt-threshold

Description: Specify whether switching to the Shortest Path Tree is enabled
             or disabled on the router. Default is 'enabled'.
```

state-refresh

- router pim state-refresh *< 10 to 300 >*

```
Usage: state-refresh <10-300>

Description: Set the interval between successive State Refresh messages
             originated by this router. Default value is 60 seconds.
```

Range: < 10 to 300 >

stub

- router ospf area *OSPF-AREA-ID* stub

```
Define a "stub" area and specify its cost.
```

Next Available Options:

- **cost** < 0 to 16777215 > -- Enter cost to use when injecting default routes into the area.**(p. 298)**
- **no-summary** -- Do not send summary LSA into the area.**(p. 303)**

- router ospf area backbone stub

```
Define a "stub" area and specify its cost.
```

Next Available Options:

- **cost** < 0 to 16777215 > -- Enter cost to use when injecting default routes into the area.**(p. 298)**
- **no-summary** -- Do not send summary LSA into the area.**(p. 303)**

transit-delay

- router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR* transit-delay *< 1 to 3600 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

- router ospf area backbone virtual-link *IP-ADDR* transit-delay *< 1 to 3600 >*

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

trap

- [no] router ospf trap *< virtual-interface-state-change | neighbor-state-change | virtual-neighbor-state-change | ... >*

```
Usage: [no] trap <TRAP-NAME|all>

Description: Enable/disable OSPF traps. The traps defined below are generated
             as the result of finding an unusual condition while parsing an
             OSPF packet or a processing a timer event. Note that if more than
             one type of unusual condition is encountered while parsing the
             packet or processing an event, only the first one will generate a
             trap. Possible trap names are:
           - 'interface-state-change' signifies that there has been a change in
             the state of a non-virtual OSPF interface. This trap is generated
             when the interface state regresses (e.g., goes from Dr to Down) or
             progresses to a terminal state (i.e., Point-to-Point, DR Other,
             Dr, or Backup).
           - 'virtual-interface-state-change' signifies the same change in the
             state of a virtual OSPF interface.
           - 'neighbor-state-change' signifies that there has been a change in
             the state of a non-virtual OSPF neighbor. This trap is generated
             when the neighbor state regresses (e.g., goes from Attempt or Full
             to 1-Way or Down) or progresses to a terminal state (e.g., 2-Way
             or Full).
           - 'virtual-neighbor-state-change' signifies the same change in the
             state of a virtual OSPF neighbor.
           - 'interface-config-error' signifies that a packet has been received
             on a non-virtual interface from a router whose configuration
             parameters conflict with this router's configuration parameters.
           - 'virtual-interface-config-error' signifies the same condition on a
             virtual interface.
           - 'interface-authentication-failure' signifies that a packet has
             been received on a non-virtual interface from a router whose
             authentication key or authentication type conflicts with this
             router's authentication key or authentication type.
           - 'virtual-interface-authentication-failure' signifies the same
             condition on a virtual interface.
           - 'interface-receive-bad-packet' signifies that an OSPF packet has
             been received on a non-virtual interface that cannot be parsed.
           - 'virtual-interface-receive-bad-packet' signifies the same
             condition on a virtual interface.
           - 'interface-retransmit-packet' signifies than an OSPF packet has
             been retransmitted on a non-virtual interface.
           - 'virtual-interface-retransmit-packet' signifies the same condition
             on a virtual interface.
           - 'originate-lsa' signifies that a new LSA has been originated by
             this router. This trap is not invoked for simple refreshes of
             LSAs, but instead will only be invoked when an LSA is
             (re)originated due to a topology change. Additionally, this trap
             does not include LSAs that are being flushed because they have
```

© 2007 Hewlett-Packard Development Company, L.P.

```
              expired.
            - 'originate-maxage-lsa' signifies that one of the LSA in the
              router's link-state database has expired.
              If 'all' is specified in place of a trap name then all the traps
              are affected by the command.
```

Supported Values:

- **virtual-interface-state-change**
- **neighbor-state-change**
- **virtual-neighbor-state-change**
- **interface-config-error**
- **virtual-interface-config-error**
- **interface-authentication-failure**
- **virtual-interface-authentication-failure**
- **interface-receive-bad-packet**
- **virtual-interface-receive-bad-packet**
- **interface-retransmit-packet**
- **virtual-interface-retransmit-packet**
- **originate-lsa**
- **originate-maxage-lsa**
- **interface-state-change**
- **all**

■ [no] router pim trap *< neighbor-loss | hardware-mrt-full | software-mrt-full | ... >*

```
Usage: [no] trap <TRAP-NAME|all>

Description: Enable/disable PIM traps. The traps defined below are generated
             as the result of finding an unusual condition or a timer event.
             Possible trap names are:

           - 'neighbor-loss' signifies that a neighbor timer expired and the
             router has no other neighbors on the same interface with a lower
             IP address than itself.

           - 'hardware-mrt-full' signifies that the MRT table is full and the
             error has been originated by hardware.

           - 'software-mrt-full' signifies that the MRT table is full and the
             error has been originated by software.

             If 'all' is specified in place of a trap name then all the traps
             are affected by the command.
```

Supported Values:

- **neighbor-loss** -- A neighbor router was lost.
- **hardware-mrt-full** -- Hardware MRT table is full.
- **software-mrt-full** -- Software MRT table is full.
- **all** -- All types of traps.

traps

■ [no] router vrrp traps

```
Usage: [no] router vrrp traps

Description: Enable/disable generation of VRRP traps. When 'enabled' an
             appropriate SNMP notification message will be sent as a result
             of finding one of the following conditions:
```

```
o 'New Master' - this trap indicates that the sending agent
                 has transitioned to 'Master' state.
o 'Authentication Failure' - this trap indicates that a packet
                 has been received from a router whose
                 authentication key or authentication type
                 conflicts with this router's authentication
                 key or authentication type.
```

type

- [no] router ospf area *OSPF-AREA-ID* range type *< summary | nssa >*

  ```
  Link state database type to apply the range.
  ```

  Supported Values:
  - **summary** -- summary.
  - **nssa** -- nssa.
- [no] router ospf area backbone range type *< summary | nssa >*

  ```
  Link state database type to apply the range.
  ```

  Supported Values:
  - **summary** -- summary.
  - **nssa** -- nssa.

virtual-link

- [no] router ospf area *OSPF-AREA-ID* virtual-link *IP-ADDR*

  ```
  Specify a virtual neighbor.
  ```

  Next Available Options:
  - **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 309)**
  - **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 306)**
  - **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 300)**
  - **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 299)**
  - **authentication-key** -- Set simple authentication method and key.**(p. 296)**
  - **authentication** -- Disable authentication.**(p. 296)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 302)**

- [no] router ospf area backbone virtual-link *IP-ADDR*

  ```
  Specify a virtual neighbor.
  ```

  Next Available Options:
  - **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 309)**
  - **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 306)**
  - **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 300)**
  - **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 299)**
  - **authentication-key** -- Set simple authentication method and key.**(p. 296)**
  - **authentication** -- Disable authentication.**(p. 296)**
  - **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 302)**

© 2007 Hewlett-Packard Development Company, L.P.

vrrp

- [no] router vrrp

```
Usage: [no] router vrrp [traps]

Description: Enable/disable/configure Virtual Router Redundancy Protocol (VRRP)
             on the device.
```

Next Available Option:

- **traps** -- Enable/disable generation of VRRP traps**(p. 311)**

© 2007 Hewlett-Packard Development Company, L.P.

setMIB

OVERVIEW

Category:	SNMP
Primary context:	manager
Related Commands	walkMIB (page 495)

```
Usage: setmib OBJECT-STR TYPE-STR VALUE-STR
              [[OBJECT-STR TYPE-STR VALUE-STR] ...]

Description: Set the value of a MIB object. The <TYPE-STR> can be:
             -i - integer
             -o - octet
             -d - object identifier
             -a - ip_addr
             -c - counter
             -g - gauge
             -t - time_ticks
             -u - unsigned integer 32
             -D - Display String
             -N - NULL
```

COMMAND STRUCTURE

- setMIB **object** -- MIB object name.instance. (ASCII-STR) **(p. 314)**
  - **type** -- Type of the value to set. See 'setmib help' for details. (ASCII-STR) **(p. 314)**
    - **value** -- A value to which to set the MIB object. (ASCII-STR) **(p. 314)**

COMMAND DETAILS

object (p. 314)	**type (p. 314)**	**value (p. 314)**

object

- setMIB *OBJECT*

```
MIB object name.instance.
```

Next Available Option:
- **type** -- Type of the value to set. See 'setmib help' for details. (ASCII-STR) **(p. 314)**

type

- setMIB *OBJECT TYPE*

```
Type of the value to set. See 'setmib help' for details.
```

Next Available Option:
- **value** -- A value to which to set the MIB object. (ASCII-STR) **(p. 314)**

value

- setMIB *OBJECT TYPE VALUE*

© 2007 Hewlett-Packard Development Company, L.P.

A value to which to set the MIB object.

© 2007 Hewlett-Packard Development Company, L.P.

setup

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	

```
Usage: setup [default-logon <CLI|Menu>]

Description: Enter the 'Switch Setup' screen for basic switch configuration.
             The optional parameter 'default-logon' changes the user
             interface presented after boot without entering full-screen
             setup.
```

COMMAND STRUCTURE

- setup **default-logon < CLI | Menu >** -- Specify whether switch should boot to CLI (default) or menu. **(p. 317)**

EXAMPLES

Example: setup

Access the Switch Setup screen to quickly configure IP addressing and other basic settings:

```
ProCurve# setup
ProCurve                                                    1-Jan-2001   2:14:27
============================- TELNET - MANAGER MODE -============================
                                  Switch Setup

  System Name : HPswitch
  System Contact : Sysadmin
  Manager Password : ************        Confirm Password : ************
  Logon Default : CLI                   Time Zone [0] : -480
  Community Name : public               Spanning Tree Enabled [No] : No

  Default Gateway : 10.10.10.1
  Time Sync Method [None] : TIMEP
  TimeP Mode [Disabled] : Disabled

  IP Config [DHCP/Bootp] : Manual
  IP Address  : 10.10.10.150
  Subnet Mask : 255.255.255.0


 Actions->   Cancel     Edit     Save     Help

Enter System Name - up to 25 characters.
Use arrow keys to change field selection, <Space> to toggle field choices,
and <Enter> to go to Actions.
```

COMMAND DETAILS

default-logon (p. 317)

© 2007 Hewlett-Packard Development Company, L.P.

default-logon

- setup default-logon *< CLI | Menu >*

```
Specify whether switch should boot to CLI (default) or menu.
```

Supported Values:

- **CLI** -- Set Command Line Interface as default console interface.
- **Menu** -- Set Menu as default console interface.

© 2007 Hewlett-Packard Development Company, L.P.

sflow

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: sflow <RECEIVER-INSTANCE> destination <IP-ADDRESS> [UDP-PORT]
       sflow <RECEIVER-INSTANCE> polling [ethernet] PORT-LIST
             <POLLING-INTERVAL>
       sflow <RECEIVER-INSTANCE> sampling [ethernet] PORT-LIST
             <SAMPLING-RATE>
       [no] sflow <RECEIVER-INSTANCE>

Description: Configure or un-claim an sflow sampling receiver.
             If the [no] option is not used, this command will
             configure the sflow sampling receiver, polling,
             and sampling.

Parameters:  IP-ADDRESS - Ip address of the sFlow
             receiver/collector/management station

             UDP-PORT - The udp application port of the sFlow
             receiver/collector/management station (default: 6343).

             POLLING-INTERVAL - The maximum interval (seconds) between
             polling of counters. (a value of 0 causes polling to be
             disabled.

             PORT-LIST - Port(s) for which packet are to be sampled.

             RECEIVER-INSTANCE - One of three posible sFlow receiver tables.

             SAMPLING-RATE - N, where 1/N is the number of packets sampled.
             (a value of 0 causes sampling to be disabled.)
```

COMMAND STRUCTURE

- [no] sflow **sflow-receiver < 1 to 3 >** -- Select one of three possible sFlow receiver tables. (NUMBER) **(p. 320)**
  - **destination** -- IP address of sFlow receiver/collector/management station. (IP-ADDR) **(p. 319)**
    - **sflow-udp-port < 1 to 65535 >** -- UDP application port of sFlow receiver/collector/management station. (NUMBER) **(p. 320)**
  - **polling** -- Specify the ports for which packets are to be polled. ([ethernet] PORT-LIST) **(p. 319)**
    - **sflow-polling-interval < 20 to 16777215 >** -- Specify the maximum interval (seconds) between polling of counters. **(p. 319)**
    - **sflow-polling-int-off < 0 >** -- Disable polling of counters. **(p. 319)**
  - **sampling** -- Specify the ports for which packets are to be sampled. ([ethernet] PORT-LIST) **(p. 319)**
    - **sflow-sampler-off < 0 >** -- Disable sampling. **(p. 320)**
    - **sflow-sampler-rate < 50 to 16441700 >** -- Specify N, where 1/N is the number of packets sampled. **(p. 320)**

© 2007 Hewlett-Packard Development Company, L.P.

COMMAND DETAILS

destination (p. 319)	sflow-polling-interval (p. 319)	sflow-sampler-off (p. 320)
polling (p. 319)	sflow-polling-int-off (p. 319)	sflow-sampler-rate (p. 320)
sampling (p. 319)	sflow-receiver (p. 320)	sflow-udp-port (p. 320)

destination

- sflow *< 1 to 3 >* destination *IP-ADDR*

```
IP address of sFlow receiver/collector/management station.
```

Next Available Option:
- **sflow-udp-port** < 1 to 65535 > -- UDP application port of sFlow receiver/collector/management station. (NUMBER) **(p. 320)**

polling

- sflow *< 1 to 3 >* polling *[ETHERNET] PORT-LIST*

```
Specify the ports for which packets are to be polled.
```

Next Available Options:
- **sflow-polling-int-off** < 0 > -- Disable polling of counters. **(p. 319)**
- **sflow-polling-interval** < 20 to 16777215 > -- Specify the maximum interval (seconds) between polling of counters. **(p. 319)**

sampling

- sflow *< 1 to 3 >* sampling *[ETHERNET] PORT-LIST*

```
Specify the ports for which packets are to be sampled.
```

Next Available Options:
- **sflow-sampler-off** < 0 > -- Disable sampling. **(p. 320)**
- **sflow-sampler-rate** < 50 to 16441700 > -- Specify N, where 1/N is the number of packets sampled. **(p. 320)**

sflow-polling-interval

- sflow *< 1 to 3 >* polling *[ETHERNET] PORT-LIST < 20 to 16777215 >*

```
Specify the maximum interval (seconds) between polling of counters.
```

Range: < 20 to 16777215 >

sflow-polling-int-off

- sflow *< 1 to 3 >* polling *[ETHERNET] PORT-LIST < 0 >*

```
Disable polling of counters.
```

Supported Values:
- **0** -- Disable polling.

© 2007 Hewlett-Packard Development Company, L.P.

sflow-receiver

- [no] sflow *< 1 to 3 >*

  ```
  Select one of three possible sFlow receiver tables.
  ```

  Range: < 1 to 3 >

  Next Available Options:
  - **destination** -- IP address of sFlow receiver/collector/management station. (IP-ADDR) **(p. 319)**
  - **polling** -- Specify the ports for which packets are to be polled. ([ethernet] PORT-LIST) **(p. 319)**
  - **sampling** -- Specify the ports for which packets are to be sampled. ([ethernet] PORT-LIST) **(p. 319)**

sflow-sampler-off

- sflow *< 1 to 3 >* sampling *[ETHERNET] PORT-LIST < 0 >*

  ```
  Disable sampling.
  ```

  Supported Values:
  - **0** -- Disable sampling.

sflow-sampler-rate

- sflow *< 1 to 3 >* sampling *[ETHERNET] PORT-LIST < 50 to 16441700 >*

  ```
  Specify N, where 1/N is the number of packets sampled.
  ```

  Range: < 50 to 16441700 >

sflow-udp-port

- sflow *< 1 to 3 >* destination *IP-ADDR < 1 to 65535 >*

  ```
  UDP application port of sFlow receiver/collector/management station.
  ```

  Range: < 1 to 65535 >

© 2007 Hewlett-Packard Development Company, L.P.

show

OVERVIEW

Category:	
Primary context:	operator
Related Commands	

```
Usage: show ...

Description: Display switch operation information.
             The 'show' must be followed by a command.
             Use 'show ?' for the list of all possible commands.
```

COMMAND STRUCTURE

- show **access-list** -- Show Access Control List information **(p. 332)**
  - **acl-name** -- Display detailed information on specified ACL. (ASCII-STR) **(p. 333)**
    - **config** -- Show all configured ACL's on the switch using the CLI syntax used to create them. **(p. 341)**
  - **config** -- Show all configured ACL's on the switch using the CLI syntax used to create them. **(p. 341)**
  - **ports** -- Show ACLs applied to the specified ports. ([ethernet] PORT-LIST) **(p. 373)**
  - **radius** -- Display ACLs applied via RADIUS. ([ethernet] PORT-LIST) **(p. 375)**
  - **resources** -- Display ACL Rules/Masks availability. **(p. 376)**
  - **vlan** -- Show ACLs applied to the specified VLAN. (VLAN-ID) **(p. 390)**
- show **accounting** -- Show Accounting configuration parameters **(p. 333)**
  - **sessions** -- Show accounting data for all active sessions **(p. 379)**
- show **arp** -- Show the IP ARP translation table **(p. 335)**
  - **vlan** -- Specify VLAN for which to show ARP entries. (VLAN-ID) **(p. 390)**
- show **arp-protect** -- Display Dynamic ARP Protection information **(p. 335)**
  - **statistics** -- (VLAN-ID-RANGE) **(p. 382)**
- show **authentication** -- Show Authentication configuration parameters **(p. 335)**
- show **authorization** -- Show Authorization configuration parameters **(p. 336)**
- show **bandwidth** -- Show queue percentages for outbound guaranteed minimum bandwidth **(p. 337)**
  - **output** -- Show outbound guaranteed minimum bandwidth. **(p. 369)**
    - **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 371)**
- show **banner** -- show the configured banner text **(p. 337)**
  - **motd** -- show the configured banner text **(p. 367)**
- show **boot-history** -- Display the system boot log **(p. 338)**
- show **cdp** -- Show CDP configuration and neighbors discovered **(p. 339)**
  - **neighbors** -- Show CDP neighbors. See 'show cdp help' for details. **(p. 368)**
    - **detail** -- Show neighbor information field-per-line instead of shortened table format. **(p. 345)**
    - **neighbors-port** -- Show CDP neighbors on specified port only. ([ethernet] PORT-NUM) **(p. 368)**
- show **config** -- Show the switch startup configuration **(p. 341)**
  - **filename < config1 >** -- Display specified configuration. **(p. 349)**
  - **files** -- List saved configuration files. **(p. 349)**
  - **status** -- Check if the running configuration differs from the statup configuration. **(p. 384)**

© 2007 Hewlett-Packard Development Company, L.P.

- show **connection-rate-filter** -- List the ports and the on/off connection-rate-filter status and sensitivity **(p. 344)**
  - **all-hosts** -- Show blocked and throttled IP addresses. **(p. 334)**
  - **blocked-hosts** -- Show blocked IP addresses. **(p. 338)**
  - **throttled-hosts** -- Show throttled IP addresses. **(p. 386)**
- show **console** -- Show serial link/console settings **(p. 344)**
- show **cpu** -- Show average CPU utilization over the last 1, 5, and 60 seconds; or the number of seconds specified **(p. 344)**
  - **slot** -- Display module CPU statistics. (SLOT-ID-RANGE) **(p. 380)**
    - **slave_time < 1 to 90 >** -- Time (seconds) over which to average CPU utilization. (NUMBER) **(p. 380)**
  - **time < 1 to 300 >** -- Time (seconds) over which to average CPU utilization. (NUMBER) **(p. 386)**
- show **crypto** -- Display flash files used for authentication **(p. 344)**
  - **client-public-key** -- Display ssh authorized client public keys. **(p. 339)**
    - **babble** -- Display phonetic hash. **(p. 337)**
    - **fingerprint** -- Display hexadecimal hash. **(p. 349)**
    - **keyfile < manager | operator >** -- Choose to display manager or operator keys. **(p. 361)**
      - **babble** -- Display phonetic hash. **(p. 337)**
      - **fingerprint** -- Display hexadecimal hash. **(p. 349)**
      - **keylist** -- Select keys to display (comma-delimited list). (ASCII-STR) **(p. 361)**
        - **babble** -- Display phonetic hash. **(p. 337)**
        - **fingerprint** -- Display hexadecimal hash. **(p. 349)**
  - **host-cert** -- Display https certificate information. **(p. 352)**
  - **host-public-key** -- Display ssh host RSA public key. **(p. 352)**
    - **babble** -- Display phonetic hash. **(p. 337)**
    - **fingerprint** -- Display hexadecimal hash. **(p. 349)**
- show **debug** -- Display currently active debug log destinations and types **(p. 345)**
- show **dhcp-relay** -- Shows the current status of DHCP Relay Agent and option 82 statistics **(p. 347)**
- show **dhcp-snooping** -- Display DHCP snooping information **(p. 347)**
  - **binding** -- Display DHCP snooping binding information. **(p. 338)**
  - **stats** -- Display DHCP snooping events. **(p. 383)**
- show **fastboot** -- Shows the current status of fastboot on switch **(p. 348)**
- show **fault-finder** -- Show the fault-finder table **(p. 349)**
- show **filter** -- Show a table of security filters or a filter detailed information, if the filter's INDEX is specified **(p. 349)**
  - **INDEX** -- Show detailed information for the filter identified by the INDEX. The indices are displayed by the 'show filter' command. **(p. 354)**
  - **source-port** -- **(p. 381)**
- show **flash** -- Show the versions of software stored in the Primary and Secondary image locations **(p. 350)**
- show **front-panel-security** -- Show current security status of the front panel butons **(p. 350)**
- show **gvrp** -- Show GVRP settings **(p. 351)**
- show **history** -- Show previously entered commands **(p. 352)**
- show **igmp** -- Show global switch IGMP configuration parameters **(p. 353)**
  - **delayed-flush** -- Shows switch-wide IGMP delayed flush value **(p. 345)**
- show **igmp-proxy** -- Show active/configured IGMP proxy forwarder information **(p. 354)**
  - **domains** -- Show all the currently configured IGMP proxy domains. **(p. 347)**
  - **entries** -- Show all the currently active IGMP proxy entries. **(p. 348)**
  - **vlans** -- Show all the VLANs currently associated with IGMP proxy domains. **(p. 391)**
- show **instrumentation** -- Show internal version-dependant counters for debugging **(p. 356)**
  - **monitor** -- Show latest values for monitored parameters **(p. 366)**
    - **configuration** -- show configured thresholds for monitored parameters **(p. 343)**
- show **interfaces** -- Show port configuration and status information **(p. 358)**

© 2007 Hewlett-Packard Development Company, L.P.

- **brief** -- Show the ports' operational parameters **(p. 338)**
  - **port-list** -- Show summary of network traffic handled by the ports ([ethernet] PORT-LIST) **(p. 371)**
- **config** -- Show configuration information **(p. 341)**
- **port-list** -- Show summary of network traffic handled by the ports ([ethernet] PORT-LIST) **(p. 371)**
  - **hc** -- Show summary of network traffic handled by the ports **(p. 352)**
- **port-utilization** -- Show the ports' bandwidth-utilization **(p. 374)**

■ show **ip** -- Show the device IP configuration **(p. 358)**

- **authorized-managers** -- Show IP addresses allowed to manage the switch **(p. 336)**
- **client-public-key** -- Show currently loaded public keys for authorized clients (NUMBER) **(p. 339)**
  - **babble** -- Display phonetic hash. **(p. 337)**
  - **fingerprint** -- Display hexadecimal hash. **(p. 349)**
- **forward-protocol** -- Show server addresses where broadcast requests received by the switch are to be forwarded based on configured port **(p. 350)**
  - **vlan** -- Specify a vlan for which to show server addresses. (VLAN-ID) **(p. 390)**
- **helper-address** -- Show DHCP servers where DHCP requests received by the switch are to be forwarded **(p. 352)**
  - **vlan** -- Specify a vlan for which to show server addresses. (VLAN-ID) **(p. 390)**
- **host-public-key** -- Display the SSH host RSA public key (NUMBER) **(p. 352)**
  - **babble** -- Display phonetic hash. **(p. 337)**
  - **fingerprint** -- Display hexadecimal hash. **(p. 349)**
- **icmp** -- Show ICMP Rate Limiting settings **(p. 353)**
- **igmp** -- Invoked without any parameters, shows per-VLAN IGMP status, or, if VLANs are disabled displays the global IGMP status **(p. 353)**
  - **config** -- Show IGMP configuration information. **(p. 341)**
  - **group** -- Show ports the specified multicast group address is registered on. (IP-ADDR) **(p. 351)**
  - **vlan** -- Show IGMP operational information for the VLAN specified. (VLAN-ID) **(p. 390)**
    - **config** -- Show IGMP configuration information for the VLAN specified. **(p. 341)**
- **irdp** -- Show IRDP (ICMP Router Discovery Protocol) settings **(p. 360)**
- **mroute** -- Show IP multicast routing table **(p. 367)**
  - **interface** -- Show IP multicast routing interfaces' information **(p. 357)**
    - **VLAN-ID** -- Specify the VLAN ID of the IP multicast routing interface to show. (VLAN-ID) **(p. 391)**
  - **IP-ADDR** -- Show detailed information for the specified entry from the IP multicast routing table (IP-ADDR) **(p. 359)**
    - **IP-ADDR** -- Specify the source IP address of the MRT entry. (IP-ADDR) **(p. 359)**
- **ospf** -- Show OSPF operational and configuration information **(p. 369)**
  - **area** -- Show OSPF areas configured on the device **(p. 334)**
    - **area-ip** -- (OSPF-AREA-ID) **(p. 335)**
  - **external-link-state** -- Show the Link State Advertisements from throughout the areas to which the device is attached **(p. 348)**
    - **advertise** -- Show each LSA as a stream of bytes in hexadecimal notation. **(p. 334)**
    - **link-state-id** -- Show LSAs with the specified ID only. (IP-ADDR) **(p. 362)**
    - **router-id** -- Show LSAs with the specified Router ID only. (IP-ADDR) **(p. 378)**
    - **sequence-number** -- Show LSAs with the specified sequence number only. **(p. 379)**
    - **status** -- The keyword is optional and can be omitted. **(p. 384)**
  - **general** -- Show OSPF basic configuration and operational information **(p. 350)**
  - **interface** -- Show OSPF interfaces' information **(p. 357)**
    - **if-ip** -- Specify IP address of the interface for which to show detailed information. (IP-ADDR) **(p. 353)**

© 2007 Hewlett-Packard Development Company, L.P.

        - **vlan** -- Specify VLAN of the interface for which to show detailed information. (VLAN-ID) **(p. 390)**
    - **link-state** -- Show all Link State Advertisements from throughout the areas to which the device is attached **(p. 362)**
        - **advertise** -- Show each LSA as a stream of bytes in hexadecimal notation. **(p. 334)**
        - **area-id** -- Show LSAs for the specified area only. (OSPF-AREA-ID) **(p. 335)**
        - **link-state-id** -- Show LSAs with the specified ID only. (IP-ADDR) **(p. 362)**
        - **router-id** -- Show LSAs with the specified Router ID only. (IP-ADDR) **(p. 378)**
        - **sequence-number** -- Show LSAs with the specified sequence number only. **(p. 379)**
        - **status** -- The keyword is optional and can be omitted. **(p. 384)**
        - **type < router | network | summary | ... >** -- Show LSAs of the specified type only. **(p. 387)**
    - **neighbor** -- Show all OSPF neighbors in the locality of of the device **(p. 368)**
        - **neighbor-ip** -- (IP-ADDR) **(p. 368)**
    - **redistribute** -- List protocols which are being redistributed into OSPF **(p. 376)**
    - **restrict** -- List routes which will not be redistributed via OSPF **(p. 376)**
    - **traps** -- Show OSPF traps enabled on the device **(p. 386)**
    - **virtual-link** -- Show status of all OSPF virtual links configured **(p. 389)**
        - **area** -- Specify area of the virtual links to show. (OSPF-AREA-ID) **(p. 334)**
        - **vlink-ip** -- Router ID of the link destination for which to show detailed information. (IP-ADDR) **(p. 391)**
    - **virtual-neighbor** -- Show all virtual neighbors of the device **(p. 389)**
        - **area** -- Specify area of the virtual neighbors to show. (OSPF-AREA-ID) **(p. 334)**
        - **vneighbor-ip** -- Router ID of the virtual neighbor for which to show detailed information. (IP-ADDR) **(p. 391)**
- **pim** -- Show PIM protocol operational and configuration information **(p. 370)**
    - **bsr** -- Show Bootstrap Router information **(p. 338)**
        - **elected** -- Show elected Bootstrap Router information. **(p. 347)**
        - **local** -- Show local Candidate-BSR configuration information. **(p. 363)**
    - **interface** -- Show PIM interface information **(p. 357)**
        - **VLAN-ID** -- Specify the VLAN ID of the PIM interface to show. (VLAN-ID) **(p. 391)**
    - **mroute** -- Show PIM-specific information from the IP multicast routing table **(p. 367)**
        - **IP-ADDR** -- Specify the IP multicast group address of the MRT entry. (IP-ADDR) **(p. 359)**
            - **IP-ADDR** -- Specify the source IP address of the MRT entry. (IP-ADDR) **(p. 359)**
    - **neighbor** -- Show PIM neighbor information **(p. 368)**
        - **IP-ADDR** -- Specify the IP address of the PIM neighbor to show. (IP-ADDR) **(p. 359)**
    - **rp-candidate** -- Show Candidate-RP operational and configuration information **(p. 378)**
        - **config** -- Show C-RP configuration information. **(p. 341)**
    - **rp-set** -- Show RP-Set information available on the router **(p. 378)**
        - **learned** -- Show RP-Set information learned from the BSR. **(p. 361)**
        - **static** -- Show statically configured RP-Set information. **(p. 382)**
- **rip** -- Show RIP operational and configuration information **(p. 377)**
    - **general** -- Show RIP basic configuration and operational information **(p. 350)**
    - **interface** -- Show RIP interfaces' information **(p. 357)**
        - **if-ip** -- Specify IP address of the interface for which to show detailed information. (IP-ADDR) **(p. 353)**
        - **vlan** -- Specify VLAN of the interface for which to show detailed information. (VLAN-ID) **(p. 390)**
    - **peer** -- Show RIP peers **(p. 370)**
        - **peer-ip** -- Specify IP address of the RIP peer to show. (IP-ADDR) **(p. 370)**
    - **redistribute** -- List protocols which are being redistributed into RIP **(p. 376)**
    - **restrict** -- List routes which will not be redistributed via RIP **(p. 376)**
- **route** -- Show the IP routing table **(p. 377)**

© 2007 Hewlett-Packard Development Company, L.P.

- ip-addr -- Destination IP address to display the routes to. (IP-ADDR) (p. 359)
- type < static | connected | rip | ... > -- Specify type of routes to display. (p. 387)
- ssh -- Show both current SSH configuration and the status of active connections (p. 382)

■ show ip-recv-mac-address -- Show VLAN L3-Mac-Address table. (p. 359)
■ show key-chain -- Display key chains (p. 360)
- CHAIN-NAME -- Show the chain detailed information. (ASCII-STR) (p. 339)

■ show lacp -- Show status of LACP trunks (p. 361)
■ show licenses -- Display license status for premium features (p. 361)
- uninstalled -- Display verification key for features which have been uninstalled. (p. 387)

■ show link-keepalive -- show link-keepalive information on the switch (p. 362)
- statistics -- show detailed statistics for all link-keepalive enabled ports. (p. 382)

■ show lldp -- Show various LLDP settings (p. 362)
- config -- Show LLDP configuration information (p. 341)
  - port-list -- Specify the port or list of ports. ([ethernet] PORT-LIST) (p. 371)
- info -- Show LLDP information about the remote or local device (p. 354)
  - local-device -- Show LLDP local device information. (p. 363)
    - port-list -- Show remote or local device information for the specified ports. ([ethernet] PORT-LIST) (p. 371)
  - remote-device -- Show LLDP remote device information. (p. 376)
    - port-list -- Show remote or local device information for the specified ports. ([ethernet] PORT-LIST) (p. 371)
- stats -- Show LLDP statistics (p. 383)
  - port-list -- Specify the port or list of ports. ([ethernet] PORT-LIST) (p. 371)

■ show lockout-mac -- Show the MAC addresses that have been locked out of the network (p. 363)
■ show logging -- Display log events (p. 363)
- -a -- Display all log events, including those from previous boot cycles. (p. 332)
- event_class < -M | -P | -W | ... > -- Specify substring to match in log entry. See 'log help' for details. (p. 348)
- option -- Filter events shown. See 'show logging help' for details. (ASCII-STR) (p. 369)
- -r -- Display log events in reverse order (most recent first). (p. 375)

■ show loop-protect -- Show loop protection status (p. 364)
- port-list -- Show loop protection summary for ports. ([ethernet] PORT-LIST) (p. 371)

■ show mac-address -- Show MAC addresses the switch has learned (p. 364)
- address-table-port -- Show MAC addresses learned on the specified ports. ([ethernet] PORT-LIST) (p. 333)
- MAC -- Show port the specified MAC address is located on. (MAC-ADDR) (p. 364)
- vlan -- Show MAC addresses learned on the specified VLAN. (VLAN-ID) (p. 390)

■ show management -- Show the switch's addresses available for management and the time server if the switch uses one (p. 365)
■ show mesh -- Show the switch mesh information such as mesh ports, adjacent switches and their peer ports (p. 365)
■ show modules -- (p. 366)
■ show monitor -- Show the switch network monitoring status and configuration, if network monitoring is enabled (p. 366)
- endpoint -- Remote mirroring destination configuration. (p. 348)
- mirror_session_id < 1 to 4 > -- Mirror destination number. (p. 366)
- name -- Mirror destination name. (p. 367)

■ show name -- Show names assigned to the ports (p. 367)
- port-list -- Show names assigned to the ports ([ethernet] PORT-LIST) (p. 371)

■ show port-access -- Show 802 (p. 371)
- -- Show Web/MAC Authentication statistics and configuration ([ethernet] PORT-LIST) (p. 331)
  - mac-based -- Show MAC Authentication statistics and configuration (p. 364)
    - clients -- Show the connected MAC address information. (p. 340)

© 2007 Hewlett-Packard Development Company, L.P.

- config -- Show the current configuration of MAC Authentication. (p. 341)
  - auth-server -- Show the authentication server-related configuration items. (p. 336)
  - detail -- Show the detailed configuration of MAC Authentication. (p. 345)
- web-based -- Show Web Authentication statistics and configuration (p. 392)
- clients -- Show the current client session statistics. (p. 340)
- config -- Show the current configuration of Web Authentication. (p. 341)
  - auth-server -- Show the authentication server-related configuration items. (p. 336)
  - detail -- Show the detailed configuration of Web Authentication. (p. 345)
  - web-server -- Show the web server-related configuration items. (p. 393)

- authenticator -- Show 802 (p. 336)
  - config -- Show 802.1x authenticator configuration. (p. 341)
  - ports -- Show information for specified ports only. ([ethernet] PORT-LIST) (p. 373)
  - session-counters -- Show 802.1x current (or last if no current sessions open) sessions counters. (p. 379)
  - statistics -- Show authentication sessions statistics for 802.1x authenticator. (p. 382)
  - vlan -- Show authorized and unauthorized vlans for 802.1x authenticator. (p. 390)
- mac-based -- Show MAC Authentication statistics and configuration (p. 364)
  - -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) (p. 331)
    - clients -- Show the connected MAC address information. (p. 340)
    - config -- Show the current configuration of MAC Authentication. (p. 341)
      - auth-server -- Show the authentication server-related configuration items. (p. 336)
      - detail -- Show the detailed configuration of MAC Authentication. (p. 345)
  - clients -- Show the connected MAC address information. (p. 340)
  - config -- Show the current configuration of MAC Authentication. (p. 341)
    - -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) (p. 331)
      - auth-server -- Show the authentication server-related configuration items. (p. 336)
      - detail -- Show the detailed configuration of MAC Authentication. (p. 345)
    - auth-server -- Show the authentication server-related configuration items. (p. 336)
- supplicant -- Show 802 (p. 384)
  - ports -- Show information for specified ports only. ([ethernet] PORT-LIST) (p. 373)
  - statistics -- Show authentication sessions statistics for 802.1x supplicant. (p. 382)
- web-based -- Show Web Authentication statistics and configuration (p. 392)
  - -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) (p. 331)
    - clients -- Show the current client session statistics. (p. 340)
    - config -- Show the current configuration of Web Authentication. (p. 341)
      - auth-server -- Show the authentication server-related configuration items. (p. 336)
      - detail -- Show the detailed configuration of Web Authentication. (p. 345)
      - web-server -- Show the web server-related configuration items. (p. 393)
  - clients -- Show the current client session statistics. (p. 340)
  - config -- Show the current configuration of Web Authentication. (p. 341)
    - -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) (p. 331)
      - auth-server -- Show the authentication server-related configuration items. (p. 336)
      - detail -- Show the detailed configuration of Web Authentication. (p. 345)
      - web-server -- Show the web server-related configuration items. (p. 393)
    - auth-server -- Show the authentication server-related configuration items. (p. 336)
    - web-server -- Show the web server-related configuration items. (p. 393)

- show port-security -- Show a table describing port security settings (p. 373)
  - intrusion-log -- Show the intrusion log records. (p. 358)
  - port-list -- Show a table describing port security settings ([ethernet] PORT-LIST) (p. 371)

© 2007 Hewlett-Packard Development Company, L.P.

- show **power-management** -- Show port power configuration and status information **(p. 374)**
  - **brief** -- Show summary of power status **(p. 338)**
    - **port-list** -- Show the ports' power status ([ethernet] PORT-LIST) **(p. 371)**
    - **slot** -- Show summary of power status (SLOT-ID-RANGE) **(p. 380)**
  - **port-list** -- Show the ports' power status ([ethernet] PORT-LIST) **(p. 371)**
- show **qos** -- Show various QoS settings **(p. 374)**
  - **device-priority** -- Show the device priority table (priority based on the IP addresses) **(p. 346)**
  - **dscp-map** -- Show mappings between DSCP policy and 802 **(p. 347)**
  - **port-priority** -- Show the port-based priority table **(p. 373)**
  - **protocol-priority** -- Show the protocol priority **(p. 374)**
  - **queue-config** -- Displays outbound port queues configuration information. **(p. 374)**
  - **resources** -- Show the qos resources **(p. 376)**
  - **tcp-udp-port-priority** -- Show TCP/UDP port priorities **(p. 385)**
  - **type-of-service** -- Show QoS priorities based on IP Type-of-Service **(p. 387)**
  - **vlan-priority** -- Show the VLAN-based priority table **(p. 391)**
- show **radius** -- Show RADIUS status and statistics information **(p. 375)**
  - **accounting** -- Show RADIUS accounting statistics **(p. 333)**
  - **authentication** -- Show RADIUS authentication statistics **(p. 335)**
  - **host** -- Show statistics information for the RADIUS host (IP-ADDR) **(p. 352)**
- show **rate-limit** -- Show rate limit maximum percentages **(p. 375)**
  - **all** -- Show limits for all traffic. **(p. 334)**
    - **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 371)**
  - **icmp** -- Show only limits for icmp traffic. **(p. 353)**
    - **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 371)**
- show **rmon** -- Show detailed rmon statistics for the ports **(p. 377)**
  - **statistics** -- Show RMON statistics for the ports ([ethernet] PORT-LIST) **(p. 382)**
- show **running-config** -- Show the switch running configuration **(p. 378)**
  - **status** -- Check if the running configuration differs from the statup configuration. **(p. 384)**
- show **sflow** -- Display information regarding the configuration, sampling, and polling with respect to 'sflow' **(p. 379)**
  - **agent** -- Displays read-only switch agent information: The agent address is normally the ip address of the first vlan configured. **(p. 334)**
  - **receiver-index < 1 to 3 >** -- Select one of the three possible sFlow receiver tables. (NUMBER) **(p. 375)**
    - **destination** -- Displays information about the receiver/collector/management-station to which the sampling-polling data is sent. **(p. 345)**
    - **sampling-polling** -- Displays information about sampling and polling. **(p. 378)**
      - **port-list** -- Displays information about sampling and polling. ([ethernet] PORT-LIST) **(p. 371)**
- show **snmp-server** -- Display information on all SNMP communities, trap receivers and Snmp response/trap source-ip policy configured on the switch **(p. 380)**
  - **community** -- Specify SNMP community to which to restrict the output. (ASCII-STR) **(p. 340)**
- show **snmpv3** -- Show configuration of SNMPv3 features. **(p. 380)**
  - **access-rights** -- Show information about access rights. **(p. 333)**
    - **group < ManagerPriv | ManagerAuth | OperatorAuth | ... >** -- Show SNMPv3 users. **(p. 351)**
      - **sec-model** -- Set security model. **(p. 379)**
        - **ver1-2c < ver1 | ver2c >** -- Configure SNMPv3 User entry. **(p. 388)**
        - **ver3** -- SNMP version 3 security model. **(p. 388)**
          - **ver3 < noauth | auth | priv >** -- Set security level. **(p. 388)**
  - **community** -- Show SNMPv3 Community table. **(p. 340)**
    - **COMMUNITY-NAME** -- Show a specific community entry. (ASCII-STR) **(p. 341)**

© 2007 Hewlett-Packard Development Company, L.P.

- **enable** -- Show SNMPv3 status. **(p. 347)**
- **engineid** -- Show switch's SNMP engineId. **(p. 348)**
- **group** -- Show SNMPv3 User to Group mappings. **(p. 351)**
  - **group < ManagerPriv | ManagerAuth | OperatorAuth | ... >** -- Show SNMPv3 users. **(p. 351)**
    - **user** -- Show a specific user. (ASCII-STR) **(p. 388)**
      - **sec-model < ver1 | ver2c | ver3 >** -- Show a specific security model. **(p. 379)**
- **notify** -- Show SNMPv3 notification table. **(p. 368)**
  - **NOTIFY-NAME** -- Show a specific notification entry. (ASCII-STR) **(p. 369)**
- **only** -- Show SNMP message reception policy. **(p. 369)**
- **params** -- Show SNMPv3 Target Parameters table. **(p. 370)**
  - **PARAM-NAME** -- Show a specific Target Parameter entry. (ASCII-STR) **(p. 370)**
- **restricted-access** -- Show SNMPv1 and SNMPv2c access properties. **(p. 376)**
- **targetaddress** -- Show SNMPv3 Target Address table. **(p. 384)**
  - **TARGETADDR-NAME** -- Show a specifc target address entry. (ASCII-STR) **(p. 385)**
- **user** -- Show SNMPv3 users. **(p. 388)**
  - **USER-NAME** -- Show a specific user. (ASCII-STR) **(p. 388)**
- **view** -- Show views. **(p. 389)**
  - **VIEW-NAME** -- Set view name. (ASCII-STR) **(p. 389)**
    - **SUB-TREE** -- Set the OID of the tree. (ASCII-STR) **(p. 384)**

■ show **sntp** -- Show configured time protocol and servers **(p. 381)**

■ show **spanning-tree** -- Show spanning tree information **(p. 381)**

- **bpdu-protection** -- Show spanning tree BPDU protection status information. **(p. 338)**
  - **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 371)**
- **config** -- Show spanning tree configuration information. **(p. 341)**
  - **instance** -- Show spanning tree instance configuration information. **(p. 354)**
    - **INSTANCE_ID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 355)**
      - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
    - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 360)**
      - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
- **instance** -- Show spanning tree instance status information. **(p. 354)**
  - **INSTANCE_ID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 355)**
    - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
  - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 360)**
    - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
- **mst-config** -- Show multiple spanning tree region configuration. **(p. 367)**
- **pending** -- Show spanning tree pending configuration **(p. 370)**
  - **instance** -- Show multiple spanning tree instance pending configuration information. **(p. 354)**
    - **INSTANCE_ID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 355)**
      - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
    - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 360)**
      - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
  - **mst-config** -- Show multiple spanning tree pending region configuration. **(p. 367)**
- **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 371)**
  - **config** -- Show spanning tree configuration information. **(p. 341)**

© 2007 Hewlett-Packard Development Company, L.P.

- **instance** -- Show spanning tree instance configuration information. **(p. 354)**
  - **INSTANCE_ID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 355)**
    - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
  - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 360)**
    - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
- **instance** -- Show spanning tree instance status information. **(p. 354)**
  - **INSTANCE_ID < 1 to 16 >** -- Spanning tree instance ID for which to show the information. **(p. 355)**
    - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**
  - **ist** -- Show the information for the internal spanning tree (IST) instance. **(p. 360)**
    - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report. **(p. 345)**

- **traps** -- Show spanning tree trap information. **(p. 386)**

- show **stack** -- Show the stack status of this switch **(p. 382)**
  - **all** -- Show information about all the stacks available on the LAN. **(p. 334)**
  - **candidates** -- Show the list of devices that are stack candidates. **(p. 339)**
  - **view** -- Show the list of devices that are stack members. **(p. 389)**
- show **static-mac** -- Show the locked-down MAC addresses in all vlans **(p. 382)**
- show **system-information** -- Show global configured and operational system parameters **(p. 384)**
- show **tacacs** -- Show TACACS status and statistics **(p. 384)**
- show **tech** -- Display output of a predefined command sequence used by technical support **(p. 385)**
  - **all** -- Display output of a predefined command sequence used by technical support **(p. 334)**
  - **buffers** -- Display output of a predefined command sequence used by technical support **(p. 339)**
  - **instrumentation** -- Display output of a predefined command sequence used by technical support **(p. 356)**
  - **mesh** -- Display output of a predefined command sequence used by technical support **(p. 365)**
  - **route** -- Display output of a predefined command sequence used by technical support **(p. 377)**
  - **statistics** -- Display output of a predefined command sequence used by technical support **(p. 382)**
  - **transceivers** -- Display output of a predefined command sequence used by technical support **(p. 386)**
- show **telnet** -- Show active incoming and outgoing sessions **(p. 385)**
- show **temperature** -- Show systems temperatures and settings **(p. 385)**
- show **terminal** -- Show logical window dimensions **(p. 386)**
- show **time** -- Show current date and time **(p. 386)**
- show **timep** -- Show configured time protocol and servers **(p. 386)**
- show **trunks** -- Show a list of ports and the trunks to which they belong **(p. 386)**
  - **port-list** -- Show the trunk information only for the ports specified. ([ethernet] PORT-LIST) **(p. 371)**
- show **uptime** -- Displays elapsed time since last boot **(p. 387)**
- show **version** -- Show software version **(p. 388)**
- show **vlans** -- Show status information for all VLANs **(p. 391)**
  - **ports** -- Show VLANs that have at least one port from the 'PORT-LIST' as a member. ([ethernet] PORT-LIST) **(p. 373)**
  - **vlan** -- Show detailed VLAN information for the VLAN with the ID supplied. (VLAN-ID) **(p. 390)**
- show **vrrp** -- Show VRRP configuration and statistics information **(p. 392)**
  - **config** -- Show VRRP configuration information for the device **(p. 341)**
    - **global** -- Show global VRRP configuration information. **(p. 350)**
  - **statistics** -- Show VRRP statistics information for the device **(p. 382)**
    - **global** -- Show global VRRP configuration information. **(p. 350)**

© 2007 Hewlett-Packard Development Company, L.P.

- vlan -- Show VRRP information for a VLAN. (p. 390)
  - VLAN-ID -- Specify VLAN for which to display VRRP information. (VLAN-ID) (p. 391)
    - config -- Show VRRP configuration information for the VLAN. (p. 341)
    - statistics -- Show VRRP statistics information for the VLAN. (p. 382)
    - vrid -- Show information for a virtual router. (p. 392)
      - VRID < 1 to 255 > -- Specify virtual router for which to display information. (p. 392)
        - config -- Show virtual router configuration information. (p. 341)
        - statistics -- Show virtual router statistics information. (p. 382)

COMMAND DETAILS

(p. 331)
-a (p. 332)
access-list (p. 332)
access-rights (p. 333)
accounting (p. 333)
acl-name (p. 333)
address-table-port (p. 333)
advertise (p. 334)
agent (p. 334)
all (p. 334)
all-hosts (p. 334)
area (p. 334)
area-id (p. 335)
area-ip (p. 335)
arp (p. 335)
arp-protect (p. 335)
authentication (p. 335)
authenticator (p. 336)
authorization (p. 336)
authorized-managers (p. 336)
auth-server (p. 336)
babble (p. 337)
bandwidth (p. 337)
banner (p. 337)
binding (p. 338)
blocked-hosts (p. 338)
boot-history (p. 338)
bpdu-protection (p. 338)
brief (p. 338)
bsr (p. 338)
buffers (p. 339)
candidates (p. 339)
cdp (p. 339)
CHAIN-NAME (p. 339)
client-public-key (p. 339)
clients (p. 340)
community (p. 340)
COMMUNITY-NAME (p. 341)
config (p. 341)
configuration (p. 343)
connection-rate-filter (p. 344)
console (p. 344)
host-cert (p. 352)
host-public-key (p. 352)
icmp (p. 353)
if-ip (p. 353)
igmp (p. 353)
igmp-proxy (p. 354)
INDEX (p. 354)
info (p. 354)
instance (p. 354)
INSTANCE_ID (p. 355)
instrumentation (p. 356)
interface (p. 357)
interfaces (p. 358)
intrusion-log (p. 358)
ip (p. 358)
ip-addr (p. 359)
IP-ADDR (p. 359)
ip-recv-mac-address (p. 359)
irdp (p. 360)
ist (p. 360)
key-chain (p. 360)
keyfile (p. 361)
keylist (p. 361)
lacp (p. 361)
learned (p. 361)
licenses (p. 361)
link-keepalive (p. 362)
link-state (p. 362)
link-state-id (p. 362)
lldp (p. 362)
local (p. 363)
local-device (p. 363)
lockout-mac (p. 363)
logging (p. 363)
loop-protect (p. 364)
MAC (p. 364)
mac-address (p. 364)
mac-based (p. 364)
management (p. 365)
mesh (p. 365)
mirror_session_id (p. 366)
modules (p. 366)
receiver-index (p. 375)
redistribute (p. 376)
remote-device (p. 376)
resources (p. 376)
restrict (p. 376)
restricted-access (p. 376)
rip (p. 377)
rmon (p. 377)
route (p. 377)
router-id (p. 378)
rp-candidate (p. 378)
rp-set (p. 378)
running-config (p. 378)
sampling-polling (p. 378)
sec-model (p. 379)
sequence-number (p. 379)
session-counters (p. 379)
sessions (p. 379)
sflow (p. 379)
slave_time (p. 380)
slot (p. 380)
snmp-server (p. 380)
snmpv3 (p. 380)
sntp (p. 381)
source-port (p. 381)
spanning-tree (p. 381)
ssh (p. 382)
stack (p. 382)
static (p. 382)
static-mac (p. 382)
statistics (p. 382)
stats (p. 383)
status (p. 384)
SUB-TREE (p. 384)
supplicant (p. 384)
system-information (p. 384)
tacacs (p. 384)
targetaddress (p. 384)
TARGETADDR-NAME (p. 385)
tcp-udp-port-priority (p. 385)
tech (p. 385)
telnet (p. 385)

© 2007 Hewlett-Packard Development Company, L.P.

cpu (p. 344)
crypto (p. 344)
debug (p. 345)
delayed-flush (p. 345)
destination (p. 345)
detail (p. 345)
device-priority (p. 346)
dhcp-relay (p. 347)
dhcp-snooping (p. 347)
domains (p. 347)
dscp-map (p. 347)
elected (p. 347)
enable (p. 347)
endpoint (p. 348)
engineid (p. 348)
entries (p. 348)
event_class (p. 348)
external-link-state (p. 348)
fastboot (p. 348)
fault-finder (p. 349)
filename (p. 349)
files (p. 349)
filter (p. 349)
fingerprint (p. 349)
flash (p. 350)
forward-protocol (p. 350)
front-panel-security (p. 350)
general (p. 350)
global (p. 350)
group (p. 351)
gvrp (p. 351)
hc (p. 352)
helper-address (p. 352)
history (p. 352)
host (p. 352)
monitor (p. 366)
motd (p. 367)
mroute (p. 367)
mst-config (p. 367)
name (p. 367)
neighbor (p. 368)
neighbor-ip (p. 368)
neighbors (p. 368)
neighbors-port (p. 368)
notify (p. 368)
NOTIFY-NAME (p. 369)
only (p. 369)
option (p. 369)
ospf (p. 369)
output (p. 369)
PARAM-NAME (p. 370)
params (p. 370)
peer (p. 370)
peer-ip (p. 370)
pending (p. 370)
pim (p. 370)
port-access (p. 371)
port-list (p. 371)
port-priority (p. 373)
ports (p. 373)
port-security (p. 373)
port-utilization (p. 374)
power-management (p. 374)
protocol-priority (p. 374)
qos (p. 374)
queue-config (p. 374)
-r (p. 375)
radius (p. 375)
rate-limit (p. 375)
temperature (p. 385)
terminal (p. 386)
throttled-hosts (p. 386)
time (p. 386)
timep (p. 386)
transceivers (p. 386)
traps (p. 386)
trunks (p. 386)
type (p. 387)
type-of-service (p. 387)
uninstalled (p. 387)
uptime (p. 387)
user (p. 388)
USER-NAME (p. 388)
ver1-2c (p. 388)
ver3 (p. 388)
version (p. 388)
view (p. 389)
VIEW-NAME (p. 389)
virtual-link (p. 389)
virtual-neighbor (p. 389)
vlan (p. 390)
VLAN-ID (p. 391)
vlan-priority (p. 391)
vlans (p. 391)
vlink-ip (p. 391)
vneighbor-ip (p. 391)
vrid (p. 392)
VRID (p. 392)
vrrp (p. 392)
web-based (p. 392)
web-server (p. 393)

- show port-access mac-based *[ETHERNET] PORT-LIST*

  `Specify ports for which MAC Authentication information will be shown.`

  Next Available Options:
  - **config** -- Show the current configuration of MAC Authentication.**(p. 341)**
  - **clients** -- Show the connected MAC address information.**(p. 340)**

- show port-access mac-based config *[ETHERNET] PORT-LIST*

  `Specify ports for which MAC Authentication information will be shown.`

  Next Available Options:
  - **auth-server** -- Show the authentication server-related configuration items.**(p. 336)**
  - **detail** -- Show the detailed configuration of MAC Authentication.**(p. 345)**

- show port-access web-based *[ETHERNET] PORT-LIST*

© 2007 Hewlett-Packard Development Company, L.P.

```
Specify ports for which Web Authentication information will be shown.
```

Next Available Options:
- **config** -- Show the current configuration of Web Authentication.**(p. 341)**
- **clients** -- Show the current client session statistics.**(p. 340)**

■ show port-access web-based config *[ETHERNET] PORT-LIST*

```
Specify ports for which Web Authentication information will be shown.
```

Next Available Options:
- **auth-server** -- Show the authentication server-related configuration items.**(p. 336)**
- **web-server** -- Show the web server-related configuration items.**(p. 393)**
- **detail** -- Show the detailed configuration of Web Authentication.**(p. 345)**

■ show port-access *[ETHERNET] PORT-LIST*

```
Usage: show port-access [PORT-LIST] <mac-based|web-based>...
       show port-access <mac-based|web-based> [PORT-LIST]...

Description: Show Web/MAC Authentication statistics and configuration. If
             PORT-LIST parameter is specified then information only for the
             specified ports is shown.
```

Next Available Options:
- **mac-based** -- Show MAC Authentication statistics and configuration**(p. 364)**
- **web-based** -- Show Web Authentication statistics and configuration**(p. 392)**

-a

■ show logging -a

```
Display all log events, including those from previous boot cycles.
```

access-list

■ show access-list

```
Usage: show access-list [config] |
                        [vlan <VLAN-ID>] |
                        [<ACL-ID> [config]]

Description: Show Access Control List information.  If no parameters
             are specified, a summary table is displayed.

Parameters:

    o config - Display all configured ACL's on the switch using
               the CLI syntax used to create them.
    o vlan <VLAN-ID> - Display Access Control Lists currently applied
                       to the specified VLAN.
    o <ACL-ID> - Display detailed information on the specified ACL.
    o resources  - Display ACL Rules/Masks availability.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **radius** -- Display ACLs applied via RADIUS. ([ethernet] PORT-LIST) **(p. 375)**
- **config** -- Show all configured ACL's on the switch using the CLI syntax used to create them. **(p. 341)**
- **vlan** -- Show ACLs applied to the specified VLAN. (VLAN-ID) **(p. 390)**
- **ports** -- Show ACLs applied to the specified ports. ([ethernet] PORT-LIST) **(p. 373)**
- **acl-name** -- Display detailed information on specified ACL. (ASCII-STR) **(p. 333)**
- **resources** -- Display ACL Rules/Masks availability.**(p. 376)**

access-rights

- show snmpv3 access-rights

```
Show information about access rights.
```

Next Available Option:

- **group** < ManagerPriv | ManagerAuth | OperatorAuth | ... > -- Show SNMPv3 users. **(p. 351)**

accounting

- show accounting

```
Usage: show accounting [sessions]

Description: Show Accounting configuration parameters.
             If 'sessions' is specified then show accounting
             data for all active sessions.
```

Next Available Option:

- **sessions** -- Show accounting data for all active sessions**(p. 379)**

- show radius accounting

```
Usage: show radius accounting

Description: Show RADIUS accounting statistics.
```

acl-name

- show access-list *ACL-NAME*

```
Display detailed information on specified ACL.
```

Next Available Option:

- **config** -- Show all configured ACL's on the switch using the CLI syntax used to create them. **(p. 341)**

address-table-port

- show mac-address *[ETHERNET] PORT-LIST*

```
Show MAC addresses learned on the specified ports.
```

© 2007 Hewlett-Packard Development Company, L.P.

advertise

- show ip ospf external-link-state advertise

```
Show each LSA as a stream of bytes in hexadecimal notation.
```

- show ip ospf link-state advertise

```
Show each LSA as a stream of bytes in hexadecimal notation.
```

agent

- show sflow agent

```
Displays read-only switch agent information: The agent address is normally the ip
address of the first vlan configured.
```

all

- show rate-limit all

```
Show limits for all traffic.
```

Next Available Option:
- **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 371)**

- show stack all

```
Show information about all the stacks available on the LAN.
```

- show tech all

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

all-hosts

- show connection-rate-filter all-hosts

```
Show blocked and throttled IP addresses.
```

area

- show ip ospf area

```
Usage: show ip ospf area [OSPF-AREA-ID]

Description: Show OSPF areas configured on the device. Invoked without
             parameters displays all OSPF areas configured. If the
             'OSPF-AREA-ID' is specified detailed information for
             the correspondent OSPF area is shown.
```

Next Available Option:
- **area-ip** -- (OSPF-AREA-ID) **(p. 335)**

- show ip ospf virtual-neighbor area *OSPF-AREA-ID*

© 2007 Hewlett-Packard Development Company, L.P.

```
Specify area of the virtual neighbors to show.
```

- show ip ospf virtual-link area *OSPF-AREA-ID*

```
Specify area of the virtual links to show.
```

area-id

- show ip ospf link-state *OSPF-AREA-ID*

```
Show LSAs for the specified area only.
```

area-ip

- show ip ospf area *OSPF-AREA-ID*

arp

- show arp

```
Usage: show arp [vlan VLAN-ID]

Description: Show the IP ARP translation table.
             If VLAN-ID is specified, the output is filtered on
             the VLAN-ID.
```

Next Available Option:

- **vlan** -- Specify VLAN for which to show ARP entries. (VLAN-ID) **(p. 390)**

arp-protect

- show arp-protect

```
Usage: show arp-protect [statistics <VLAN-ID_RANGE>]

Description: Display the current configuration of dynamice ARP
             protection, including validation checks and trusted
             ports.
             o statistics - Displays statistics about forwarded
               ARP packets, dropped ARP packets, MAC validation
               failure, and IP validation failures. You can enter
               a range of VLAN IDs for which to display statistics,
               for example, 1-20.
```

Next Available Option:

- **statistics** -- Display ARP protection VLAN counters. **(p. 382)**

authentication

- show authentication

```
Usage: show authentication

Description: Show Authentication configuration parameters.
```

- show radius authentication

```
Usage: show radius authentication

Description: Show RADIUS authentication statistics.
```

© 2007 Hewlett-Packard Development Company, L.P.

authenticator

- show port-access authenticator

```
Usage: show port-access authenticator [config|statistics|session-counters]

Description: Show 802.1x (Port Based Network Access) authenticator
             current status, configuration or last session counters.
```

Next Available Options:

- **ports** -- Show information for specified ports only. ([ethernet] PORT-LIST) **(p. 373)**
- **config** -- Show 802.1x authenticator configuration.**(p. 341)**
- **statistics** -- Show authentication sessions statistics for 802.1x authenticator.**(p. 382)**
- **session-counters** -- Show 802.1x current (or last if no current sessions open) sessions counters.**(p. 379)**
- **vlan** -- Show authorized and unauthorized vlans for 802.1x authenticator.**(p. 390)**

authorization

- show authorization

```
Usage: show authorization

Description: Show Authorization configuration parameters.
```

authorized-managers

- show ip authorized-managers

```
Usage: show ip authorized-managers

Description: Show IP addresses allowed to manage the switch.
```

auth-server

- show port-access mac-based *[ETHERNET] PORT-LIST* config auth-server

```
Show the authentication server-related configuration items.
```

- show port-access mac-based config *[ETHERNET] PORT-LIST* auth-server

```
Show the authentication server-related configuration items.
```

- show port-access mac-based config auth-server

```
Show the authentication server-related configuration items.
```

- show port-access web-based *[ETHERNET] PORT-LIST* config auth-server

```
Show the authentication server-related configuration items.
```

- show port-access web-based config *[ETHERNET] PORT-LIST* auth-server

```
Show the authentication server-related configuration items.
```

- show port-access web-based config auth-server

```
Show the authentication server-related configuration items.
```

- show port-access *[ETHERNET] PORT-LIST* mac-based config auth-server

© 2007 Hewlett-Packard Development Company, L.P.

```
Show the authentication server-related configuration items.
```

- show port-access *[ETHERNET] PORT-LIST* web-based config auth-server

```
Show the authentication server-related configuration items.
```

babble

- show crypto client-public-key babble

```
Display phonetic hash.
```

- show crypto client-public-key *< manager | operator >* babble

```
Display phonetic hash.
```

- show crypto client-public-key *< manager | operator > KEYLIST* babble

```
Display phonetic hash.
```

- show crypto host-public-key babble

```
Display phonetic hash.
```

- show ip client-public-key babble

```
Display phonetic hash.
```

- show ip host-public-key babble

```
Display phonetic hash.
```

bandwidth

- show bandwidth

```
Usage: show bandwidth <output> [PORT-LIST]

Description: Show queue percentages for outbound guaranteed minimum
             bandwidth. If PORT-LIST parameter is specified, information
             is shown only for the specified ports.
```

Next Available Option:

- **output** -- Show outbound guaranteed minimum bandwidth.**(p. 369)**

banner

- show banner

```
Usage: show banner motd

Description: show the configured banner text.
```

Next Available Option:

- **motd** -- show the configured banner text**(p. 367)**

© 2007 Hewlett-Packard Development Company, L.P.

binding

- show dhcp-snooping binding

```
Display DHCP snooping binding information.
```

blocked-hosts

- show connection-rate-filter blocked-hosts

```
Show blocked IP addresses.
```

boot-history

- show boot-history

```
Usage: show boot-history

Description: Display the system boot log.
```

bpdu-protection

- show spanning-tree bpdu-protection

```
Show spanning tree BPDU protection status information.
```

Next Available Option:

- **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 371)**

brief

- show interfaces brief

```
Usage: show interfaces brief

Description: Show the ports' operational parameters.
```

Next Available Option:

- **port-list** -- Show summary of network traffic handled by the ports ([ethernet] PORT-LIST) **(p. 371)**

- show power-management brief

```
Usage: show power-management brief

Description: Show summary of power status.
```

Next Available Options:

- **port-list** -- Show the ports' power status ([ethernet] PORT-LIST) **(p. 371)**
- **slot** -- Show summary of power status (SLOT-ID-RANGE) **(p. 380)**

bsr

- show ip pim bsr

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: show ip pim bsr [elected|local]

Description: Show Bootstrap Router information. When invoked without parameters
             displays the information about currently elected BSR and the local
             Candidate-BSR and Candidate-RP information.
```

Next Available Options:

- **elected** -- Show elected Bootstrap Router information. **(p. 347)**
- **local** -- Show local Candidate-BSR configuration information. **(p. 363)**

buffers

- show tech buffers

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Displays buffer contents of switch.
```

candidates

- show stack candidates

```
Show the list of devices that are stack candidates.
```

cdp

- show cdp

```
Usage: show cdp [neighbor [PORT-NUM] [detail]]

Description: Show CDP configuration and neighbors discovered.
             Legend for 'capability' field of the 'show cdp neighbor'
             command output:
             R - Performs level 3 routing for at least one network
                 layer protocol.
             B - Performs level 2 transparent bridging.
             Bs - Performs level 2 source-route bridging.
             S - Performs level 2 switching.
             P - Sends and receives packets for at least one network
                 layer protocol.
             In - The bridge or switch does not forward IGMP Report packets.
             L1 - Provides level 1 functionality.
```

Next Available Option:

- **neighbors** -- Show CDP neighbors. See 'show cdp help' for details.**(p. 368)**

CHAIN-NAME

- show key-chain *CHAIN-NAME*

```
Show the chain detailed information.
```

client-public-key

- show crypto client-public-key

© 2007 Hewlett-Packard Development Company, L.P.

```
Display ssh authorized client public keys.
```

Next Available Options:
- **babble** -- Display phonetic hash.**(p. 337)**
- **fingerprint** -- Display hexadecimal hash.**(p. 349)**
- **keyfile** < manager | operator > -- Choose to display manager or operator keys.**(p. 361)**

- show ip client-public-key

```
Usage: show ip client-public-key [babble|fingerprint]

Description: Show currently loaded public keys for authorized clients.
             The 'babble' and 'fingerprint' options produce a phonetic or
             hexadecimal hash instead of displaying the raw key file.
```

Next Available Options:
- **babble** -- Display phonetic hash.**(p. 337)**
- **fingerprint** -- Display hexadecimal hash.**(p. 349)**

clients

- show port-access mac-based *[ETHERNET] PORT-LIST* clients

```
Show the connected MAC address information.
```

- show port-access mac-based clients

```
Show the connected MAC address information.
```

- show port-access web-based *[ETHERNET] PORT-LIST* clients

```
Show the current client session statistics.
```

- show port-access web-based clients

```
Show the current client session statistics.
```

- show port-access *[ETHERNET] PORT-LIST* mac-based clients

```
Show the connected MAC address information.
```

- show port-access *[ETHERNET] PORT-LIST* web-based clients

```
Show the current client session statistics.
```

community

- show snmp-server *COMMUNITY*

```
Specify SNMP community to which to restrict the output.
```

- show snmpv3 community

```
Show SNMPv3 Community table.
```

Next Available Option:
- **COMMUNITY-NAME** -- Show a specific community entry. (ASCII-STR) **(p. 341)**

© 2007 Hewlett-Packard Development Company, L.P.

COMMUNITY-NAME

- show snmpv3 community *COMMUNITY-NAME*

```
Show a specific community entry.
```

config

- show access-list config

```
Show all configured ACL's on the switch using
                            the CLI syntax used to create them.
```

- show access-list *ACL-NAME* config

```
Show all configured ACL's on the switch using
                            the CLI syntax used to create them.
```

- show config

```
Usage: show config [files | FILENAME | status]

Description: Show the switch startup configuration.

Parameters:

    o files - list switch configuration files.  Shows which file is active
              and which are associated with primary and secondary images.
    o FILENAME - show specified configuration instead of active configuration.
    o status - check if there are changes in running configuration not
              saved to the startup configuration file.
```

Next Available Options:

- **status** -- Check if the running configuration differs from the statup configuration.**(p. 384)**
- **files** -- List saved configuration files.**(p. 349)**
- **filename** < config > -- Display specified configuration.**(p. 349)**

- show interfaces config

```
Usage: show interfaces config

Description: Show configuration information.
```

- show ip igmp *VLAN-ID* config

```
Show IGMP configuration information for the VLAN specified.
```

- show ip igmp config

```
Show IGMP configuration information.
```

- show ip pim rp-candidate config

```
Show C-RP configuration information.
```

- show lldp config

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: show lldp config [[ethernet] PORT-LIST]]

Description: Show LLDP configuration information.
    o [ethernet] PORT-LIST - Show port configuration information.
```

Next Available Option:

- **port-list** -- Specify the port or list of ports. ([ethernet] PORT-LIST) **(p. 371)**

- show port-access authenticator config

```
Show 802.1x authenticator configuration.
```

- show port-access mac-based *[ETHERNET] PORT-LIST* config

```
Show the current configuration of MAC Authentication.
```

Next Available Options:

- **auth-server** -- Show the authentication server-related configuration items.**(p. 336)**
- **detail** -- Show the detailed configuration of MAC Authentication.**(p. 345)**

- show port-access mac-based config

```
Show the current configuration of MAC Authentication.
```

Next Available Options:

- -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 331)**
- **auth-server** -- Show the authentication server-related configuration items.**(p. 336)**

- show port-access web-based *[ETHERNET] PORT-LIST* config

```
Show the current configuration of Web Authentication.
```

Next Available Options:

- **auth-server** -- Show the authentication server-related configuration items.**(p. 336)**
- **web-server** -- Show the web server-related configuration items.**(p. 393)**
- **detail** -- Show the detailed configuration of Web Authentication.**(p. 345)**

- show port-access web-based config

```
Show the current configuration of Web Authentication.
```

Next Available Options:

- -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) **(p. 331)**
- **auth-server** -- Show the authentication server-related configuration items.**(p. 336)**
- **web-server** -- Show the web server-related configuration items.**(p. 393)**

- show port-access *[ETHERNET] PORT-LIST* mac-based config

```
Show the current configuration of MAC Authentication.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **auth-server** -- Show the authentication server-related configuration items.**(p. 336)**
- **detail** -- Show the detailed configuration of MAC Authentication.**(p. 345)**

■ show port-access *[ETHERNET] PORT-LIST* web-based config

```
Show the current configuration of Web Authentication.
```

Next Available Options:
- **auth-server** -- Show the authentication server-related configuration items.**(p. 336)**
- **web-server** -- Show the web server-related configuration items.**(p. 393)**
- **detail** -- Show the detailed configuration of Web Authentication.**(p. 345)**

■ show spanning-tree *[ETHERNET] PORT-LIST* config

```
Show spanning tree configuration information.
```

Next Available Option:
- **instance** -- Show spanning tree instance configuration information.**(p. 354)**

■ show spanning-tree config

```
Show spanning tree configuration information.
```

Next Available Option:
- **instance** -- Show spanning tree instance configuration information.**(p. 354)**

■ show vrrp config

```
Usage: show vrrp config

Description: Show VRRP configuration information for the device.
```

Next Available Option:
- **global** -- Show global VRRP configuration information. **(p. 350)**

■ show vrrp vlan *VLAN-ID* config

```
Show VRRP configuration information for the VLAN.
```

■ show vrrp vlan *VLAN-ID* vrid *< 1 to 255 >* config

```
Show virtual router configuration information.
```

configuration

■ show instrumentation monitor configuration

```
Usage: show instrumentation monitor configuration

Description: show configured thresholds for monitored parameters.
             shows the parameter name and the configured threshold
             value for all parameters.
             If instrumenation monitoring for the particular paramter
```

```
                is disabled then threshold for the particular parameter is
                displayed as 'Not Monitored'.
```

connection-rate-filter

- show connection-rate-filter

```
Usage: show connection-rate-filter [all-hosts] [blocked-hosts] [throttled-hosts]

Description: List the ports and the on/off connection-rate-filter status and
             sensitivity.

Parameters:
    o all-hosts       - Display the IP addresses of the hosts that are blocked
                        and throttled
    o blocked-hosts   - Print the IP addresses of the hosts that are currently
                        blocked
    o throttled-hosts - Print the IP addresses of the hosts that are currently
                        throttled
```

Next Available Options:

- **all-hosts** -- Show blocked and throttled IP addresses.**(p. 334)**
- **blocked-hosts** -- Show blocked IP addresses.**(p. 338)**
- **throttled-hosts** -- Show throttled IP addresses.**(p. 386)**

console

- show console

```
Usage: show console

Description: Show serial link/console settings.
```

cpu

- show cpu

```
Usage: show cpu [<1-300>]
                [slot <SLOT-LIST> [<1-90>] ]

Description: Show average CPU utilization over the last 1, 5, and 60 seconds;
             or the number of seconds specified.

             Use the 'slot' argument to display CPU utilization for the
             specified modules, rather than the chassis CPU.
```

Next Available Options:

- **time** < 1 to 300 > -- Time (seconds) over which to average CPU utilization. (NUMBER) **(p. 386)**
- **slot** -- Display module CPU statistics. (SLOT-ID-RANGE) **(p. 380)**

crypto

- show crypto

```
Usage: show crypto client-public-key [INDEX] [<fingerprint|babble>]
                  host-public-key [<fingerprint|babble>]
                  host-cert
```

© 2007 Hewlett-Packard Development Company, L.P.

```
Description: Display flash files used for authentication.

Parameters:

    o client-public-key - display keys used by ssh for client public
            key authentication.
    o INDEX - specify a single client public key, with more detailed
            output.
    o <fingerprint|babble> - display a hexadecimal or phonetic hash
            of the key[s].
    o host-public-key - display the ssh host public key.
    o host-cert - display the device's ssl host certificate.
```

Next Available Options:

- **client-public-key** -- Display ssh authorized client public keys.**(p. 339)**
- **host-public-key** -- Display ssh host RSA public key.**(p. 352)**
- **host-cert** -- Display https certificate information.**(p. 352)**

debug

- show debug

```
Usage: show debug

Description: Display currently active debug log destinations and types.
```

delayed-flush

- show igmp delayed-flush

```
Usage: show igmp delayed-flush

Description: Shows switch-wide IGMP delayed flush value.
```

destination

- show sflow *< 1 to 3 >* destination

```
Displays information about the receiver/collector/management-station to which the
sampling-polling data is sent.
```

detail

- show cdp neighbors detail

```
Show neighbor information field-per-line instead of shortened table format.
```

- show port-access mac-based *[ETHERNET] PORT-LIST* config detail

```
Show the detailed configuration of MAC Authentication.
```

- show port-access mac-based config *[ETHERNET] PORT-LIST* detail

```
Show the detailed configuration of MAC Authentication.
```

- show port-access web-based *[ETHERNET] PORT-LIST* config detail

```
Show the detailed configuration of Web Authentication.
```

© 2007 Hewlett-Packard Development Company, L.P.

- show port-access web-based config *[ETHERNET] PORT-LIST* detail

  Show the detailed configuration of Web Authentication.

- show port-access *[ETHERNET] PORT-LIST* mac-based config detail

  Show the detailed configuration of MAC Authentication.

- show port-access *[ETHERNET] PORT-LIST* web-based config detail

  Show the detailed configuration of Web Authentication.

- show spanning-tree *[ETHERNET] PORT-LIST* config instance ist detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree *[ETHERNET] PORT-LIST* config instance *< 1 to 16 >* detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree *[ETHERNET] PORT-LIST* detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree *[ETHERNET] PORT-LIST* instance ist detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree *[ETHERNET] PORT-LIST* instance *< 1 to 16 >* detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree config instance ist detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree config instance *< 1 to 16 >* detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree instance ist detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree instance *< 1 to 16 >* detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree pending instance ist detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

- show spanning-tree pending instance *< 1 to 16 >* detail

  Show spanning tree extended details Port, Bridge, Rx, and Tx report.

device-priority

- show qos device-priority

```
Usage: show qos device-priority

Description: Show the device priority table (priority based on
             the IP addresses).
```

dhcp-relay

- show dhcp-relay

```
Usage: show dhcp-relay

Description: Shows the current status of DHCP Relay Agent and
             option 82 statistics.
```

dhcp-snooping

- show dhcp-snooping

```
Usage: show dhcp-snooping [<binding|stats>]

Description: Display DHCP snooping information.

Parameters:

            o binding - Display DHCP snooping binding information.

            o stats   - Display DHCP snooping events.
```

Next Available Options:

- **binding** -- Display DHCP snooping binding information.**(p. 338)**
- **stats** -- Display DHCP snooping events.**(p. 383)**

domains

- show igmp-proxy domains

```
Show all the currently configured IGMP proxy domains.
```

dscp-map

- show qos dscp-map

```
Usage: qos dscp-map

Description: Show mappings between DSCP policy and 802.1p priority.
```

elected

- show ip pim bsr elected

```
Show elected Bootstrap Router information.
```

enable

- show snmpv3 enable

```
Show SNMPv3 status.
```

© 2007 Hewlett-Packard Development Company, L.P.

endpoint

- show monitor endpoint

```
Remote mirroring destination configuration.
```

engineid

- show snmpv3 engineid

```
Show switch's SNMP engineId.
```

entries

- show igmp-proxy entries

```
Show all the currently active IGMP proxy entries.
```

event_class

- show logging

```
Specify substring to match in log entry. See 'log help' for details.
```

Supported Values:

- **-M** -- Major event class.
- **-P** -- Performance event class.
- **-W** -- Warning event class.
- **-I** -- Information event class.
- **-D** -- Debug event class.

external-link-state

- show ip ospf external-link-state

```
Usage: show ip ospf external-link-state [status|advertise]

Description: Show the Link State Advertisements from throughout
             the areas to which the device is attached. The command
             shows only External Link State Advertisements.
             The 'status' keyword is optional and does not affect the
             command output. If the 'advertise' is specified, each LSA
             is shown as a stream of bytes in hexadecimal notation.
```

Next Available Options:

- **status** -- The keyword is optional and can be omitted.**(p. 384)**
- **advertise** -- Show each LSA as a stream of bytes in hexadecimal notation.**(p. 334)**
- **link-state-id** -- Show LSAs with the specified ID only. (IP-ADDR) **(p. 362)**
- **router-id** -- Show LSAs with the specified Router ID only. (IP-ADDR) **(p. 378)**
- **sequence-number** -- Show LSAs with the specified sequence number only.**(p. 379)**

fastboot

- show fastboot

```
Usage: show fastboot

Description: Shows the current status of fastboot on switch.
```

© 2007 Hewlett-Packard Development Company, L.P.

fault-finder

- show fault-finder

```
Usage: show fault-finder

Description: Show the fault-finder table.
```

filename

- show config *< config >*

```
Display specified configuration.
```

Supported Values:
- **config**

files

- show config files

```
List saved configuration files.
```

filter

- show filter

```
Usage: show filter [INDEX]

Description: Show a table of security filters or a filter
             detailed information, if the filter's INDEX is specified.
```

Next Available Options:
- **INDEX** -- Show detailed information for the filter identified by the INDEX. The indices are displayed by the 'show filter' command.**(p. 354)**
- **source-port** -- **(p. 381)**

fingerprint

- show crypto client-public-key fingerprint

```
Display hexadecimal hash.
```

- show crypto client-public-key *< manager | operator >* fingerprint

```
Display hexadecimal hash.
```

- show crypto client-public-key *< manager | operator > KEYLIST* fingerprint

```
Display hexadecimal hash.
```

- show crypto host-public-key fingerprint

```
Display hexadecimal hash.
```

- show ip client-public-key fingerprint

```
Display hexadecimal hash.
```

- show ip host-public-key fingerprint

© 2007 Hewlett-Packard Development Company, L.P.

```
Display hexadecimal hash.
```

flash

- show flash

```
Usage: show flash

Description: Show the versions of software stored in the Primary
             and Secondary image locations.
```

forward-protocol

- show ip forward-protocol

```
Usage: show ip forward-protocol [vlan <VLAN-ID>]

Description: Show server addresses where broadcast requests received by the
             switch are to be forwarded based on configured port.
```

Next Available Option:

- **vlan** -- Specify a vlan for which to show server addresses. (VLAN-ID) **(p. 390)**

front-panel-security

- show front-panel-security

```
Usage: show front-panel-security

Description: Show current security status of the front panel butons.  If
             'password-clear' is disabled, the password(s) cannot be reset using
             the clear button on the front panel of the device.  If 'factory-
             reset' is disabled, the configuation/password(s) can not be reset
             using the clear and reset button combination at boot time.  With
             'password-recovery' enabled (and the front panel buttons disabled),
             a lost password can be recovered by contacting HP customer support.
             With 'password-recovery' disabled, there is no way to access a
             device after losing a password with the front panel buttons
             disabled.
```

general

- show ip ospf general

```
Usage: show ip ospf general

Description: Show OSPF basic configuration and operational information.
```

- show ip rip general

```
Usage: show ip rip general

Description: Show RIP basic configuration and operational information.
```

global

- show vrrp config global

```
Show global VRRP configuration information.
```

© 2007 Hewlett-Packard Development Company, L.P.

- show vrrp statistics global

  Show global VRRP configuration information.

group

- show ip igmp group *IP-ADDR*

  Show ports the specified multicast group address is registered on.

- show snmpv3 access-rights *< ManagerPriv | ManagerAuth | OperatorAuth | ... >*

  Show SNMPv3 users.

  Supported Values:
  - **ManagerPriv** -- Require privacy and authentication, can access all objects.
  - **ManagerAuth** -- Require authentication, can access all objects.
  - **OperatorAuth** -- Requires authentication, limited access to objects.
  - **OperatorNoAuth** -- No authentication required, limited access to objects.
  - **ComManagerRW** -- Community with manager and unrestricted write access.
  - **ComManagerR** -- Community with manager and restricted write access.
  - **ComOperatorRW** -- Community with operator and unrestricted write access.
  - **ComOperatorR** -- Community with operator and restricted write access.

  Next Available Option:
  - **sec-model** -- Set security model. **(p. 379)**

- show snmpv3 group

  Show SNMPv3 User to Group mappings.

  Next Available Option:
  - **group** < ManagerPriv | ManagerAuth | OperatorAuth | ... > -- Show SNMPv3 users. **(p. 351)**

- show snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >*

  Show SNMPv3 users.

  Supported Values:
  - **ManagerPriv** -- Require privacy and authentication, can access all objects.
  - **ManagerAuth** -- Require authentication, can access all objects.
  - **OperatorAuth** -- Requires authentication, limited access to objects.
  - **OperatorNoAuth** -- No authentication required, limited access to objects.
  - **ComManagerRW** -- Community with manager and unrestricted write access.
  - **ComManagerR** -- Community with manager and restricted write access.
  - **ComOperatorRW** -- Community with operator and unrestricted write access.
  - **ComOperatorR** -- Community with operator and restricted write access.

  Next Available Option:
  - **user** -- Show a specific user. (ASCII-STR) **(p. 388)**

gvrp

- show gvrp

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: show gvrp

Description: Show GVRP settings.
```

hc

- show interfaces *[ETHERNET] PORT-LIST* hc

```
Usage: show interfaces [ethernet] PORT-LIST

Description: Show summary of network traffic handled by the ports.
```

helper-address

- show ip helper-address

```
Usage: show ip helper-address [vlan <VLAN-ID>]

Description: Show DHCP servers where DHCP requests received by the
             switch are to be forwarded.
```

Next Available Option:

- **vlan** -- Specify a vlan for which to show server addresses. (VLAN-ID) **(p. 390)**

history

- show history

```
Usage: show history

Description: Show previously entered commands.
```

host

- show radius host *IP-ADDR*

```
Usage: show radius host <IP-ADDR>

Description: Show statistics information for the RADIUS host.
```

host-cert

- show crypto host-cert

```
Display https certificate information.
```

host-public-key

- show crypto host-public-key

```
Display ssh host RSA public key.
```

Next Available Options:

- **babble** -- Display phonetic hash.**(p. 337)**
- **fingerprint** -- Display hexadecimal hash.**(p. 349)**

- show ip host-public-key

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: show ip host-public-key [babble|fingerprint]

Description: Display the SSH host RSA public key.  The 'babble' and
             'fingerprint' options display a phonetic or hexadecimal
             hash instead of displaying the numeric values.
```

Next Available Options:
- **babble** -- Display phonetic hash.**(p. 337)**
- **fingerprint** -- Display hexadecimal hash.**(p. 349)**

icmp

- show ip icmp

```
Usage: show ip icmp

Description: Show ICMP Rate Limiting settings.
```

- show rate-limit icmp

```
Show only limits for icmp traffic.
```

Next Available Option:
- **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 371)**

if-ip

- show ip ospf interface *IP-ADDR*

```
Specify IP address of the interface for which to show detailed information.
```

- show ip rip interface *IP-ADDR*

```
Specify IP address of the interface for which to show detailed information.
```

igmp

- show igmp

```
Usage: show igmp [...]

Description: Show global switch IGMP configuration parameters.
             To get a list of all possible parameters use 'show igmp ?'.
```

Next Available Option:
- **delayed-flush** -- Shows switch-wide IGMP delayed flush value**(p. 345)**

- show ip igmp

```
Usage: show ip igmp [config|group IP-ADDR|VLAN-ID [config]]

Description: Invoked without any parameters, shows per-VLAN IGMP status,
             or, if VLANs are disabled displays the global IGMP status.
             When followed by the 'config' keyword, shows IGMP global
             configuration information. VLAN-ID can be used to get
             operational and configuration information for a particular
```

© 2007 Hewlett-Packard Development Company, L.P.

```
VLAN, if VLAN support is enabled. The 'group' keyword can be
used to show a list of ports where a particular multicast group
is registered.
```

Next Available Options:

- **vlan** -- Show IGMP operational information for the VLAN specified. (VLAN-ID) **(p. 390)**
- **config** -- Show IGMP configuration information.**(p. 341)**
- **group** -- Show ports the specified multicast group address is registered on. (IP-ADDR) **(p. 351)**

igmp-proxy

- show igmp-proxy

```
Usage: show igmp-proxy <entries|domains|vlans>

Description: Show active/configured IGMP proxy forwarder information.
             When followed by the 'entries' keyword, shows all currently
             active IGMP proxy entries. The 'domains' keyword can be
             used to show all the currently configured IGMP proxy
             domains. The 'vlans' keyword can be used to show all the
             VLANs currently associated with IGMP proxy domains.
```

Next Available Options:

- **entries** -- Show all the currently active IGMP proxy entries.**(p. 348)**
- **domains** -- Show all the currently configured IGMP proxy domains.**(p. 347)**
- **vlans** -- Show all the VLANs currently associated with IGMP proxy domains.**(p. 391)**

INDEX

- show filter *INTEGER*

```
Show detailed information for the filter identified by the INDEX.
The indices are displayed by the 'show filter' command.
```

info

- show lldp info

```
Usage: show lldp info <local-device | remote device> [PORT-LIST]

Description: Show LLDP information about the remote or local device.
   o [ethernet] PORT-LIST - Show local or remote device information
                            for the specified ports.
```

Next Available Options:

- **remote-device** -- Show LLDP remote device information.**(p. 376)**
- **local-device** -- Show LLDP local device information.**(p. 363)**

instance

- show spanning-tree *[ETHERNET] PORT-LIST* config instance

```
Show spanning tree instance configuration information.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 360)**
- **INSTANCE_ID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 355)**

■ show spanning-tree *[ETHERNET] PORT-LIST* instance

```
Show spanning tree instance status information.
```

Next Available Options:
- **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 360)**
- **INSTANCE_ID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 355)**

■ show spanning-tree config instance

```
Show spanning tree instance configuration information.
```

Next Available Options:
- **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 360)**
- **INSTANCE_ID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 355)**

■ show spanning-tree instance

```
Show spanning tree instance status information.
```

Next Available Options:
- **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 360)**
- **INSTANCE_ID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 355)**

■ show spanning-tree pending instance

```
Show multiple spanning tree instance pending configuration information.
```

Next Available Options:
- **ist** -- Show the information for the internal spanning tree (IST) instance.**(p. 360)**
- **INSTANCE_ID** < 1 to 16 > -- Spanning tree instance ID for which to show the information.**(p. 355)**

INSTANCE_ID

■ show spanning-tree *[ETHERNET] PORT-LIST* config instance *< 1 to 16 >*

```
Spanning tree instance ID for which to show the information.
```

Range: < 1 to 16 >

Next Available Option:
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

© 2007 Hewlett-Packard Development Company, L.P.

- show spanning-tree *[ETHERNET] PORT-LIST* instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

  Range: < 1 to 16 >

  Next Available Option:
  - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

- show spanning-tree config instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

  Range: < 1 to 16 >

  Next Available Option:
  - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

- show spanning-tree instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

  Range: < 1 to 16 >

  Next Available Option:
  - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

- show spanning-tree pending instance *< 1 to 16 >*

  ```
  Spanning tree instance ID for which to show the information.
  ```

  Range: < 1 to 16 >

  Next Available Option:
  - **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

instrumentation

- show instrumentation

  ```
  Usage: show instrumentation

  Description: Show internal version-dependant counters for debugging.
  This data is for factory troubleshooting purposes.  The data displayed
  is dependent on which version of code is running.

  Data is maintained for the current 5 minutes, hour, and day.  At the end of
  every 5 minutes, hour, or day, averages and min/max values are calculated
  and the current interval's data is copied to the previous interval's data.
  For example, the previous day's data is updated at midnight local time. The
  previous hour's data is updated on the hour.

  There are many situations in which data is not yet available, or data is
  not maintained.  In this case, an asterisk is displayed.  It is never an
  error condition.
  ```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **monitor** -- Show latest values for monitored parameters**(p. 366)**

■ show tech instrumentation

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

interface

■ show ip ospf interface

```
Usage: show ip ospf interface [IP-ADDR|vlan VLAN-ID]

Description: Show OSPF interfaces' information. Invoked without
             parameters shows all OSPF interfaces configured. If the
             'IP-ADDR' or the VLAN is specified detailed information
             for the interface determined through the parameter is shown.
```

Next Available Options:
- **vlan** -- Specify VLAN of the interface for which to show detailed information. (VLAN-ID) **(p. 390)**
- **if-ip** -- Specify IP address of the interface for which to show detailed information. (IP-ADDR) **(p. 353)**

■ show ip rip interface

```
Usage: show ip rip interface [IP-ADDR|vlan VLAN-ID]

Description: Show RIP interfaces' information. Invoked without
             parameters shows all RIP interfaces configured. If the
             'IP-ADDR' or the VLAN is specified detailed information
             for the interface determined through the parameter is shown.
```

Next Available Options:
- **vlan** -- Specify VLAN of the interface for which to show detailed information. (VLAN-ID) **(p. 390)**
- **if-ip** -- Specify IP address of the interface for which to show detailed information. (IP-ADDR) **(p. 353)**

■ show ip mroute interface

```
Usage: show ip mroute interface [VLAN-ID]

Description: Show IP multicast routing interfaces' information. Invoked
             without parameters shows all IP multicast routing interfaces.
             If the VLAN-ID is specified then detailed information for the
             specified interface is shown.
```

Next Available Option:
- **VLAN-ID** -- Specify the VLAN ID of the IP multicast routing interface to show. (VLAN-ID) **(p. 391)**

■ show ip pim interface

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: show ip pim interface [VLAN-ID]

Description: Show PIM interface information. Invoked without parameters
             shows all enabled PIM routing interfaces. If the VLAN-ID is
             specified then detailed information for the specified interface
             is shown.
```

Next Available Option:

- **VLAN-ID** -- Specify the VLAN ID of the PIM interface to show. (VLAN-ID) **(p. 391)**

interfaces

- show interfaces

```
Usage: show interfaces [config|brief|[ethernet] PORT-LIST|port-utilization]

Description: Show port configuration and status information.

     o config    - Show configuration information.
     o brief     - Show the ports' operational parameters.
     o [ethernet] PORT-LIST - Show summary of network traffic
                  handled by the ports.
     o port-utilization     - Show the ports' bandwidth-utilization.
```

Next Available Options:

- **port-list** -- Show summary of network traffic handled by the ports ([ethernet] PORT-LIST) **(p. 371)**
- **config** -- Show configuration information**(p. 341)**
- **brief** -- Show the ports' operational parameters**(p. 338)**
- **port-utilization** -- Show the ports' bandwidth-utilization**(p. 374)**

intrusion-log

- show port-security intrusion-log

```
Show the intrusion log records.
```

ip

- show ip

```
Usage: show ip [...]

Description: Show the device IP configuration. Invoked without parameters
             shows IP configuration for the switch or all VLANs. When
             followed by a parameter displays information for a particular
             IP protocol or feature. To get a list of all possible
             parameters use 'show ip ?'.
```

Next Available Options:

- **authorized-managers** -- Show IP addresses allowed to manage the switch**(p. 336)**
- **client-public-key** -- Show currently loaded public keys for authorized clients (NUMBER) **(p. 339)**
- **helper-address** -- Show DHCP servers where DHCP requests received by the switch are to be forwarded**(p. 352)**
- **forward-protocol** -- Show server addresses where broadcast requests received by the switch are to be forwarded based on configured port**(p. 350)**

© 2007 Hewlett-Packard Development Company, L.P.

- **icmp** -- Show ICMP Rate Limiting settings**(p. 353)**
- **host-public-key** -- Display the SSH host RSA public key (NUMBER) **(p. 352)**
- **igmp** -- Invoked without any parameters, shows per-VLAN IGMP status, or, if VLANs are disabled displays the global IGMP status**(p. 353)**
- **irdp** -- Show IRDP (ICMP Router Discovery Protocol) settings**(p. 360)**
- **ospf** -- Show OSPF operational and configuration information**(p. 369)**
- **rip** -- Show RIP operational and configuration information**(p. 377)**
- **route** -- Show the IP routing table**(p. 377)**
- **ssh** -- Show both current SSH configuration and the status of active connections**(p. 382)**
- **mroute** -- Show IP multicast routing table**(p. 367)**
- **pim** -- Show PIM protocol operational and configuration information**(p. 370)**

ip-addr

- show ip route *IP-ADDR*

```
Destination IP address to display the routes to.
```

IP-ADDR

- show ip mroute *IP-ADDR*

```
Usage: show ip mroute [GRP-ADDR SRC-ADDR]

Description: Show detailed information for the specified entry from the IP
             multicast routing table. GRP-ADDR is the IP multicast group
             address and SRC-ADDR is the source IP address of the entry.
```

Next Available Option:

- **IP-ADDR** -- Specify the source IP address of the MRT entry. (IP-ADDR) **(p. 359)**

- show ip mroute *IP-ADDR IP-ADDR*

```
Specify the source IP address of the MRT entry.
```

- show ip pim mroute *IP-ADDR*

```
Specify the IP multicast group address of the MRT entry.
```

Next Available Option:

- **IP-ADDR** -- Specify the source IP address of the MRT entry. (IP-ADDR) **(p. 359)**

- show ip pim mroute *IP-ADDR IP-ADDR*

```
Specify the source IP address of the MRT entry.
```

- show ip pim neighbor *IP-ADDR*

```
Specify the IP address of the PIM neighbor to show.
```

ip-recv-mac-address

- show ip-recv-mac-address

```
Show VLAN L3-Mac-Address table.
```

© 2007 Hewlett-Packard Development Company, L.P.

irdp

- show ip irdp

```
Usage: show ip irdp

Description: Show IRDP (ICMP Router Discovery Protocol) settings.
```

ist

- show spanning-tree *[ETHERNET] PORT-LIST* config instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

Next Available Option:
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

- show spanning-tree *[ETHERNET] PORT-LIST* instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

Next Available Option:
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

- show spanning-tree config instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

Next Available Option:
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

- show spanning-tree instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

Next Available Option:
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

- show spanning-tree pending instance ist

```
Show the information for the internal spanning tree (IST) instance.
```

Next Available Option:
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**

key-chain

- show key-chain

```
Usage: show key-chain [CHAN-NAME-STR]

Description: Display key chains. The command displays a list of key chains
             configured. If a key chain name is specified the command shows
             the chain keys and information of routing protocols configured
             to use the chain.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **CHAIN-NAME** -- Show the chain detailed information. (ASCII-STR) **(p. 339)**

keyfile

- show crypto client-public-key *< manager | operator >*

```
Choose to display manager or operator keys.
```

Supported Values:
- **manager** -- Select manager public keys.
- **operator** -- Select operator public keys.

Next Available Options:
- **babble** -- Display phonetic hash.**(p. 337)**
- **fingerprint** -- Display hexadecimal hash.**(p. 349)**
- **keylist** -- Select keys to display (comma-delimited list). (ASCII-STR) **(p. 361)**

keylist

- show crypto client-public-key *< manager | operator > KEYLIST*

```
Select keys to display (comma-delimited list).
```

Next Available Options:
- **babble** -- Display phonetic hash.**(p. 337)**
- **fingerprint** -- Display hexadecimal hash.**(p. 349)**

lacp

- show lacp

```
Usage: show lacp

Description: Show status of LACP trunks.
```

learned

- show ip pim rp-set learned

```
Show RP-Set information learned from the BSR.
```

licenses

- show licenses

```
Usage: show licenses [uninstalled]

Description: Display license status for premium features.  Use 'uninstalled'
             to display the uninstall verification key for features which
             have been uninstalled.
```

Next Available Option:
- **uninstalled** -- Display verification key for features which have been uninstalled. **(p. 387)**

© 2007 Hewlett-Packard Development Company, L.P.

link-keepalive

- show link-keepalive

```
Usage: show link-keepalive [statistics]

Description: show link-keepalive information on the switch.
             'show link-keepalive' command displays all the ports that are
             enabled for link-keepalive. 'show link-keepalive statistics'
             command displays detailed statistics like UDLD packets sent,
             UDLD packets received etc for all link-keepalive enabled ports.
```

Next Available Option:

- **statistics** -- show detailed statistics for all link-keepalive enabled ports.**(p. 382)**

link-state

- show ip ospf link-state

```
Usage: show ip ospf link-state [OSPF-AREA-ID] [status|advertise]

Description: Show all Link State Advertisements from throughout
             the areas to which the device is attached.
             The 'status' keyword is optional and does not affect the
             command output. If the 'advertise' is specified, each LSA
             is shown as a stream of bytes in hexadecimal notation.
```

Next Available Options:

- **area-id** -- Show LSAs for the specified area only. (OSPF-AREA-ID) **(p. 335)**
- **advertise** -- Show each LSA as a stream of bytes in hexadecimal notation.**(p. 334)**
- **link-state-id** -- Show LSAs with the specified ID only. (IP-ADDR) **(p. 362)**
- **router-id** -- Show LSAs with the specified Router ID only. (IP-ADDR) **(p. 378)**
- **sequence-number** -- Show LSAs with the specified sequence number only.**(p. 379)**
- **status** -- The keyword is optional and can be omitted.**(p. 384)**
- **type** < router | network | summary | ... > -- Show LSAs of the specified type only.**(p. 387)**

link-state-id

- show ip ospf external-link-state link-state-id *IP-ADDR*

```
Show LSAs with the specified ID only.
```

- show ip ospf link-state link-state-id *IP-ADDR*

```
Show LSAs with the specified ID only.
```

lldp

- show lldp

```
Usage: show lldp ...

Description: Show various LLDP settings. Use 'show lldp ?' for the
             list of all possible options.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:
- **config** -- Show LLDP configuration information**(p. 341)**
- **info** -- Show LLDP information about the remote or local device**(p. 354)**
- **stats** -- Show LLDP statistics**(p. 383)**

local

- show ip pim bsr local

```
Show local Candidate-BSR configuration information.
```

local-device

- show lldp info local-device

```
Show LLDP local device information.
```

Next Available Option:
- **port-list** -- Show remote or local device information for the specified ports. ([ethernet] PORT-LIST) **(p. 371)**

lockout-mac

- show lockout-mac

```
Usage: show lockout-mac

Description: Show the MAC addresses that have been locked out
             of the network.
```

logging

- show logging

```
Usage: show logging [-a|-r|-m|-p|-w|-i|-d|substring ...]

Description: Display log events.
             -a - Instructs the switch to display all recorded log
             events, which includes events from previous boot cycles.
             -r - Instructs the switch to display recorded
             log events in reverse order (most recent first).
             substring - Instructs the switch to display
             only those events that match the substring.

             The remaining event class options (listed below in
             order of severity - lowest severity first) confine
             output to event clases of equal or higher severity
             -d - Debug
             -i - Informative
             -w - Warnings
             -p - Performance
             -m - Major
             Only one of options -d,-i,-w,-p and -m may be specified.

             The -a, -r, and substring options may be used in
             combination with an event class option.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:

- **option** -- Filter events shown. See 'show logging help' for details. (ASCII-STR) **(p. 369)**
- **-a** -- Display all log events, including those from previous boot cycles.**(p. 332)**
- **-r** -- Display log events in reverse order (most recent first).**(p. 375)**
- **event_class** < -M | -P | -W | ... > -- Specify substring to match in log entry. See 'log help' for details.**(p. 348)**

loop-protect

- show loop-protect

```
Usage: show loop-protect [ethernet] PORT-LIST
Description: Show loop protection status. if no PORT-LIST is specified, then
             information is shown only for the ports that have loop protection
             enabled.
```

Next Available Option:

- **port-list** -- Show loop protection summary for ports. ([ethernet] PORT-LIST) **(p. 371)**

MAC

- show mac-address *MAC-ADDR*

```
Show port the specified MAC address is located on.
```

mac-address

- show mac-address

```
Usage: show mac-address [[ethernet] PORT-LIST|vlan VLAN-ID|MAC-ADDR]

Description: Show MAC addresses the switch has learned.
             You can display addresses learned on a particular port,
             a PORT-LIST, a VLAN-ID, or a particular MAC address.
```

Next Available Options:

- **address-table-port** -- Show MAC addresses learned on the specified ports. ([ethernet] PORT-LIST) **(p. 333)**
- **vlan** -- Show MAC addresses learned on the specified VLAN. (VLAN-ID) **(p. 390)**
- **MAC** -- Show port the specified MAC address is located on. (MAC-ADDR) **(p. 364)**

mac-based

- show port-access mac-based

```
Usage: show port-access [PORT-LIST] mac-based
                        [<config [auth-server|detail]>|clients]
       show port-access mac-based [PORT-LIST]
                        [<config [auth-server|detail]>|clients]
       show port-access mac-based config [PORT-LIST] [auth-server|detail]

Description: Show MAC Authentication statistics and configuration. If
             PORT-LIST parameter has been specified then information only
             for the specified ports is shown.
             If 'config' keyword has been specified then the configuration
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                of MAC Authentication is shown.
                If 'auth-server' keyword has been specified then the
                authentication server-related configuration items are shown.
                If PORT-LIST and 'detail' keyword has been specified then the
                detailed configuration of MAC Authentication for the specified
                ports is shown.
                If 'clients' keyword has been specified then the connected MAC
                address information is shown.
```

Next Available Options:

- -- Specify ports for which MAC Authentication information will be shown. ([ethernet] PORT-LIST) (p. 331)
- **config** -- Show the current configuration of MAC Authentication.(p. 341)
- **clients** -- Show the connected MAC address information.(p. 340)

■ show port-access *[ETHERNET] PORT-LIST* mac-based

```
Usage: show port-access [PORT-LIST] mac-based
                        [<config [auth-server|detail]>|clients]
       show port-access mac-based [PORT-LIST]
                        [<config [auth-server|detail]>|clients]
       show port-access mac-based config [PORT-LIST] [auth-server|detail]

Description: Show MAC Authentication statistics and configuration. If
             PORT-LIST parameter has been specified then information only
             for the specified ports is shown.
             If 'config' keyword has been specified then the configuration
             of MAC Authentication is shown.
             If 'auth-server' keyword has been specified then the
             authentication server-related configuration items are shown.
             If PORT-LIST and 'detail' keyword has been specified then the
             detailed configuration of MAC Authentication for the specified
             ports is shown.
             If 'clients' keyword has been specified then the connected MAC
             address information is shown.
```

Next Available Options:

- **config** -- Show the current configuration of MAC Authentication.(p. 341)
- **clients** -- Show the connected MAC address information.(p. 340)

management

■ show management

```
Usage: show management

Description: Show the switch's addresses available for management
             and the time server if the switch uses one.
```

mesh

■ show mesh

```
Usage: show mesh

Description: Show the switch mesh information such as mesh
             ports, adjacent switches and their peer ports.
```

© 2007 Hewlett-Packard Development Company, L.P.

- show tech mesh

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

mirror_session_id

- show monitor *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

modules

- show modules

```
Usage: show modules

Description: Show installed modules information
```

monitor

- show instrumentation monitor

```
Usage: show instrumentation monitor

Description: Show latest values for monitored parameters.
The data displayed is dependent on which version of code is running.

Data is maintained for the current 5 minutes, hour, and day.  At the end of
every 5 minutes, hour, or day, averages and min/max values are calculated
and the current interval's data is copied to the previous interval's data.
For example, the previous day's data is updated at midnight local time. The
previous hour's data is updated on the hour.

There are many situations in which data is not yet available, or data is
not maintained.  In this case, an asterisk is displayed.  It is never an
error condition.
```

Next Available Option:

- **configuration** -- show configured thresholds for monitored parameters**(p. 343)**

- show monitor

```
Usage: show monitor

Description: Show the switch network monitoring status and
             configuration, if network monitoring is enabled.
```

Next Available Options:

- **mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 366)**
- **name** -- Mirror destination name.**(p. 367)**
- **endpoint** -- Remote mirroring destination configuration.**(p. 348)**

© 2007 Hewlett-Packard Development Company, L.P.

motd

- show banner motd

```
Usage: show banner motd

Description: show the configured banner text.
```

mroute

- show ip mroute

```
Usage: show ip mroute [command]

Description: Show IP multicast routing table. The 'command' can be used to
             obtain more detailed information of the IP multicast routing
             functionality. Use 'show ip mroute ?' to get a list of all
             possible commands.
```

Next Available Options:

- **IP-ADDR** -- Show detailed information for the specified entry from the IP multicast routing table (IP-ADDR) **(p. 359)**
- **interface** -- Show IP multicast routing interfaces' information**(p. 357)**

- show ip pim mroute

```
Usage: show ip pim mroute [GRP-ADDR SRC-ADDR]

Description: Show PIM-specific information from the IP multicast routing
             table. Invoked without parameters shows all PIM entries from
             the IP MRT. If multicast group address and source address are
             specified then detailed information for the specified entry is
             shown.
```

Next Available Option:

- **IP-ADDR** -- Specify the IP multicast group address of the MRT entry. (IP-ADDR) **(p. 359)**

mst-config

- show spanning-tree mst-config

```
Show multiple spanning tree region configuration.
```

- show spanning-tree pending mst-config

```
Show multiple spanning tree pending region configuration.
```

name

- show monitor name

```
Mirror destination name.
```

- show name

```
Usage: show name [[ethernet] PORT-LIST]
```

© 2007 Hewlett-Packard Development Company, L.P.

```
Description: Show names assigned to the ports. If the PORT-LIST is not
             specified the default is to list all of the ports.
```

Next Available Option:
- **port-list** -- Show names assigned to the ports ([ethernet] PORT-LIST) **(p. 371)**

neighbor

- show ip ospf neighbor

```
Usage: show ip ospf neighbor [IP-ADDR]

Description: Show all OSPF neighbors in the locality of of the
             device. The 'IP-ADDR' can be specified to retrieve
             detailed information for the specific neighbor only.
```

Next Available Option:
- **neighbor-ip** -- (IP-ADDR) **(p. 368)**

- show ip pim neighbor

```
Usage: show ip pim neighbor [IP-ADDR]

Description: Show PIM neighbor information. Invoked without parameters
             shows all PIM neighbors of this device. If the IP-ADDR is
             specified then detailed information for the specified neighbor
             is shown.
```

Next Available Option:
- **IP-ADDR** -- Specify the IP address of the PIM neighbor to show. (IP-ADDR) **(p. 359)**

neighbor-ip

- show ip ospf neighbor *IP-ADDR*

neighbors

- show cdp neighbors

```
Show CDP neighbors. See 'show cdp help' for details.
```

Next Available Options:
- **neighbors-port** -- Show CDP neighbors on specified port only. ([ethernet] PORT-NUM) **(p. 368)**
- **detail** -- Show neighbor information field-per-line instead of shortened table format.**(p. 345)**

neighbors-port

- show cdp neighbors *[ETHERNET] PORT-NUM*

```
Show CDP neighbors on specified port only.
```

notify

- show snmpv3 notify

© 2007 Hewlett-Packard Development Company, L.P.

```
Show SNMPv3 notification table.
```

Next Available Option:
- **NOTIFY-NAME** -- Show a specific notification entry. (ASCII-STR) **(p. 369)**

NOTIFY-NAME

- show snmpv3 notify *NOTIFY-NAME*

```
Show a specific notification entry.
```

only

- show snmpv3 only

```
Show SNMP message reception policy.
```

option

- show logging *OPTION*

```
Filter events shown. See 'show logging help' for details.
```

ospf

- show ip ospf

```
Usage: show ip ospf [command]

Description: Show OSPF operational and configuration information.
             The 'command' can be used to obtain more detailed information
             of the protocol functionality. Use 'show ip ospf ?' to get a
             list of all possible commands.
```

Next Available Options:
- **general** -- Show OSPF basic configuration and operational information**(p. 350)**
- **area** -- Show OSPF areas configured on the device**(p. 334)**
- **external-link-state** -- Show the Link State Advertisements from throughout the areas to which the device is attached**(p. 348)**
- **interface** -- Show OSPF interfaces' information**(p. 357)**
- **link-state** -- Show all Link State Advertisements from throughout the areas to which the device is attached**(p. 362)**
- **neighbor** -- Show all OSPF neighbors in the locality of of the device**(p. 368)**
- **redistribute** -- List protocols which are being redistributed into OSPF**(p. 376)**
- **restrict** -- List routes which will not be redistributed via OSPF**(p. 376)**
- **traps** -- Show OSPF traps enabled on the device**(p. 386)**
- **virtual-neighbor** -- Show all virtual neighbors of the device**(p. 389)**
- **virtual-link** -- Show status of all OSPF virtual links configured**(p. 389)**

output

- show bandwidth output

```
Show outbound guaranteed minimum bandwidth.
```

Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **port-list** -- Specify ports for which information will be shown. ([ethernet] PORT-LIST) **(p. 371)**

PARAM-NAME

- show snmpv3 params *PARAM-NAME*

```
Show a specific Target Parameter entry.
```

params

- show snmpv3 params

```
Show SNMPv3 Target Parameters table.
```

Next Available Option:

- **PARAM-NAME** -- Show a specific Target Parameter entry. (ASCII-STR) **(p. 370)**

peer

- show ip rip peer

```
Usage: show ip rip peer [IP-ADDR]

Description: Show RIP peers. Invoked without parameters shows all RIP
             peers of the device. If 'IP-ADDR' is specified only
             the peer having the address is displayed.
```

Next Available Option:

- **peer-ip** -- Specify IP address of the RIP peer to show. (IP-ADDR) **(p. 370)**

peer-ip

- show ip rip peer *IP-ADDR*

```
Specify IP address of the RIP peer to show.
```

pending

- show spanning-tree pending

```
Usage: show spanning-tree pending ...

Description: Show spanning tree pending configuration.
             Use 'show spanning-tree pending ?' to see a list of all
             available options.
```

Next Available Options:

- **mst-config** -- Show multiple spanning tree pending region configuration.**(p. 367)**
- **instance** -- Show multiple spanning tree instance pending configuration information.**(p. 354)**

pim

- show ip pim

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: show ip pim [command]

Description: Show PIM protocol operational and configuration information.
             The 'command' can be used to obtain more detailed information
             of the protocol functionality. Use 'show ip pim ?' to get a
             list of all possible commands.
```

Next Available Options:

- **mroute** -- Show PIM-specific information from the IP multicast routing table**(p. 367)**
- **interface** -- Show PIM interface information**(p. 357)**
- **neighbor** -- Show PIM neighbor information**(p. 368)**
- **bsr** -- Show Bootstrap Router information**(p. 338)**
- **rp-candidate** -- Show Candidate-RP operational and configuration information**(p. 378)**
- **rp-set** -- Show RP-Set information available on the router**(p. 378)**

port-access

- show port-access

```
Usage: show port-access <authenticator [...] | supplicant [...]>

Description: Show 802.1x (Port Based Network Access) supplicant or
             authenticator current status and configuration.
```

Next Available Options:

- **authenticator** -- Show 802**(p. 336)**
- **supplicant** -- Show 802**(p. 384)**
- **mac-based** -- Show MAC Authentication statistics and configuration**(p. 364)**
- **web-based** -- Show Web Authentication statistics and configuration**(p. 392)**
- -- Show Web/MAC Authentication statistics and configuration ([ethernet] PORT-LIST) **(p. 331)**

port-list

- show interfaces *[ETHERNET] PORT-LIST*

```
Usage: show interfaces [ethernet] PORT-LIST

Description: Show summary of network traffic handled by the ports.
```

Next Available Option:

- **hc** -- Show summary of network traffic handled by the ports**(p. 352)**

- show interfaces brief *[ETHERNET] PORT-LIST*

```
Usage: show interfaces [ethernet] PORT-LIST

Description: Show summary of network traffic handled by the ports.
```

- show lldp config *[ETHERNET] PORT-LIST*

```
Specify the port or list of ports.
```

- show lldp info remote-device *[ETHERNET] PORT-LIST*

© 2007 Hewlett-Packard Development Company, L.P.

```
Show remote or local device information for the
                                    specified ports.
```

- show lldp info local-device *[ETHERNET] PORT-LIST*

```
Show remote or local device information for the
                                    specified ports.
```

- show lldp stats *[ETHERNET] PORT-LIST*

```
Specify the port or list of ports.
```

- show loop-protect *[ETHERNET] PORT-LIST*

```
Show loop protection summary for ports.
```

- show name *[ETHERNET] PORT-LIST*

```
Usage: show name [[ethernet] PORT-LIST]

Description: Show names assigned to the ports. If the PORT-LIST is not
             specified the default is to list all of the ports.
```

- show port-security *[ETHERNET] PORT-LIST*

```
Usage: show port-security [intrusion-log|[ethernet] PORT-LIST]

Description: Show a table describing port security settings.

    o intrusion-log - Show the intrusion log records.
    o PORT-LIST     - Show detailed information on particular ports in the
                      PORT-LIST specified.
```

- show power-management *[ETHERNET] PORT-LIST*

```
Usage: show power-management [ethernet] PORT-LIST

Description: Show the ports' power status.
```

- show power-management brief *[ETHERNET] PORT-LIST*

```
Usage: show power-management [ethernet] PORT-LIST

Description: Show the ports' power status.
```

- show bandwidth output *[ETHERNET] PORT-LIST*

```
Specify ports for which information will be shown.
```

- show rate-limit icmp *[ETHERNET] PORT-LIST*

```
Specify ports for which information will be shown.
```

- show rate-limit all *[ETHERNET] PORT-LIST*

```
Specify ports for which information will be shown.
```

- show sflow *< 1 to 3 >* sampling-polling *[ETHERNET] PORT-LIST*

```
Displays information about sampling and polling.
```

- show spanning-tree *[ETHERNET] PORT-LIST*

© 2007 Hewlett-Packard Development Company, L.P.

```
Limit the port information printed to the set of the specified ports.
```

Next Available Options:
- **config** -- Show spanning tree configuration information.**(p. 341)**
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**
- **instance** -- Show spanning tree instance status information.**(p. 354)**

- show spanning-tree bpdu-protection *[ETHERNET] PORT-LIST*

```
Limit the port information printed to the set of the specified ports.
```

- show trunks *[ETHERNET] PORT-LIST*

```
Show the trunk information only for the ports specified.
```

port-priority

- show qos port-priority

```
Usage: show qos port-priority

Description: Show the port-based priority table.
```

ports

- show access-list ports *[ETHERNET] PORT-LIST*

```
Show ACLs applied to the specified ports.
```

- show port-access authenticator *[ETHERNET] PORT-LIST*

```
Show information for specified ports only.
```

- show port-access supplicant *[ETHERNET] PORT-LIST*

```
Show information for specified ports only.
```

- show vlans ports *[ETHERNET] PORT-LIST*

```
Show VLANs that have at least one port from the 'PORT-LIST' as a member.
```

port-security

- show port-security

```
Usage: show port-security [intrusion-log|[ethernet] PORT-LIST]

Description: Show a table describing port security settings.

    o intrusion-log - Show the intrusion log records.
    o PORT-LIST     - Show detailed information on particular ports in the
                      PORT-LIST specified.
```

Next Available Options:
- **port-list** -- Show a table describing port security settings ([ethernet] PORT-LIST) **(p. 371)**
- **intrusion-log** -- Show the intrusion log records.**(p. 358)**

© 2007 Hewlett-Packard Development Company, L.P.

port-utilization

- show interfaces port-utilization

```
Usage: show interfaces port-utilization

Description: Show the ports' bandwidth-utilization.
```

power-management

- show power-management

```
Usage: show power-management [brief|[ethernet] PORT-LIST]

Description: Show port power configuration and status information.

     o brief     - Show summary of power status.
     o [ethernet] PORT-LIST - Show the ports' power status.
```

Next Available Options:

- **port-list** -- Show the ports' power status ([ethernet] PORT-LIST) **(p. 371)**
- **brief** -- Show summary of power status**(p. 338)**

protocol-priority

- show qos protocol-priority

```
Usage: show qos protocol

Description: Show the protocol priority.
```

qos

- show qos

```
Usage: show qos ...

Description: Show various QoS settings. Use 'show qos ?' for the
             list of all possible options.
```

Next Available Options:

- **device-priority** -- Show the device priority table (priority based on the IP addresses)**(p. 346)**
- **dscp-map** -- Show mappings between DSCP policy and 802**(p. 347)**
- **port-priority** -- Show the port-based priority table**(p. 373)**
- **protocol-priority** -- Show the protocol priority**(p. 374)**
- **tcp-udp-port-priority** -- Show TCP/UDP port priorities**(p. 385)**
- **type-of-service** -- Show QoS priorities based on IP Type-of-Service**(p. 387)**
- **vlan-priority** -- Show the VLAN-based priority table**(p. 391)**
- **resources** -- Show the qos resources**(p. 376)**
- **queue-config** -- Displays outbound port queues configuration information. **(p. 374)**

queue-config

- show qos queue-config

```
Displays outbound port queues configuration information.
```

© 2007 Hewlett-Packard Development Company, L.P.

-r

- show logging -r

```
Display log events in reverse order (most recent first).
```

radius

- show access-list radius *[ETHERNET] PORT-LIST*

```
Display ACLs applied via RADIUS.
```

- show radius

```
Usage: show radius [authentication|accounting|host <IP-ADDR>]

Description: Show RADIUS status and statistics information. Invoked without
             parameters shows general RADIUS configuration for the switch.

    o authentication - show RADIUS authentication statistics information.

    o accounting     - show RADIUS accounting statistics information.

    o host <IP-ADDR> - show comprehensive statistics information for the host.
```

Next Available Options:

- **authentication** -- Show RADIUS authentication statistics**(p. 335)**
- **accounting** -- Show RADIUS accounting statistics**(p. 333)**
- **host** -- Show statistics information for the RADIUS host (IP-ADDR) **(p. 352)**

rate-limit

- show rate-limit

```
Usage: show rate-limit <all|icmp> [PORT-LIST]

Description: Show rate limit maximum percentages. If PORT-LIST parameter is
             specified, information is shown only for the specified ports.

             Use 'all' to show limits applied to all traffic, or 'icmp' to
             show limits for ICMP traffic only.
```

Next Available Options:

- **icmp** -- Show only limits for icmp traffic.**(p. 353)**
- **all** -- Show limits for all traffic.**(p. 334)**

receiver-index

- show sflow *< 1 to 3 >*

```
Select one of the three possible sFlow receiver tables.
```

Range: < 1 to 3 >

Next Available Options:

- **destination** -- Displays information about the receiver/collector/management-station to which the sampling-polling data is sent.**(p. 345)**

© 2007 Hewlett-Packard Development Company, L.P.

- **sampling-polling** -- Displays information about sampling and polling.**(p. 378)**

redistribute

- show ip ospf redistribute

```
Usage: show ip ospf redistribute

Description: List protocols which are being redistributed into OSPF.
```

- show ip rip redistribute

```
Usage: show ip rip redistribute

Description: List protocols which are being redistributed into RIP.
```

remote-device

- show lldp info remote-device

```
Show LLDP remote device information.
```

Next Available Option:

- **port-list** -- Show remote or local device information for the specified ports. ([ethernet] PORT-LIST) **(p. 371)**

resources

- show access-list resources

```
Display ACL Rules/Masks availability.
```

- show qos resources

```
Usage: show qos resources

Description: Show the qos resources.
```

restrict

- show ip ospf restrict

```
Usage: show ip ospf restrict

Description: List routes which will not be redistributed via OSPF.
```

- show ip rip restrict

```
Usage: show ip rip restrict

Description: List routes which will not be redistributed via RIP.
```

restricted-access

- show snmpv3 restricted-access

```
Show SNMPv1 and SNMPv2c access properties.
```

© 2007 Hewlett-Packard Development Company, L.P.

rip

- show ip rip

```
Usage: show ip rip [command]

Description: Show RIP operational and configuration information.
             The 'command' can be used to obtain more detailed information
             of the protocol functionality. Use 'show ip rip ?' to get a
             list of all possible commands.
```

Next Available Options:

- **general** -- Show RIP basic configuration and operational information**(p. 350)**
- **interface** -- Show RIP interfaces' information**(p. 357)**
- **peer** -- Show RIP peers**(p. 370)**
- **redistribute** -- List protocols which are being redistributed into RIP**(p. 376)**
- **restrict** -- List routes which will not be redistributed via RIP**(p. 376)**

rmon

- show rmon

```
Usage: show rmon statistics PORT-LIST

Description: Show detailed rmon statistics for the ports.

     o statistics PORT-LIST - Show statistics measured by the
                   probe for the ports.
```

Next Available Option:

- **statistics** -- Show RMON statistics for the ports ([ethernet] PORT-LIST) **(p. 382)**

route

- show ip route

```
Usage: show ip route [IP-ADDR] [static|connected|rip|ospf]

Description: Show the IP routing table.
             The output may be restricted to a specific destination or
             type of route.
```

Next Available Options:

- **ip-addr** -- Destination IP address to display the routes to. (IP-ADDR) **(p. 359)**
- **type** < static | connected | rip | ... > -- Specify type of routes to display.**(p. 387)**

- show tech route

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

© 2007 Hewlett-Packard Development Company, L.P.

router-id

- show ip ospf external-link-state router-id *IP-ADDR*

```
Show LSAs with the specified Router ID only.
```

- show ip ospf link-state router-id *IP-ADDR*

```
Show LSAs with the specified Router ID only.
```

rp-candidate

- show ip pim rp-candidate

```
Usage: show ip pim rp-candidate [config]

Description: Show Candidate-RP operational and configuration information.
             When invoked without parameter shows current operational status
             of the Candidate-RP.
```

Next Available Option:

- **config** -- Show C-RP configuration information. **(p. 341)**

rp-set

- show ip pim rp-set

```
Usage: show ip pim rp-set [static|learned]

Description: Show RP-Set information available on the router.
             When invoked without parameters shows all statically configured
             and dynamically learned entries. If keyword 'static' is specified
             the information about statically configured entries is shown.
             If keyword 'learned' is specified the information learned from
             the BSR is shown.
```

Next Available Options:

- **static** -- Show statically configured RP-Set information. **(p. 382)**
- **learned** -- Show RP-Set information learned from the BSR. **(p. 361)**

running-config

- show running-config

```
Usage: show running-config [status]

Description: Show the switch running configuration. If the status
             keyword is specified check if there are changes in running
             configuration not saved to startup configuration file.
```

Next Available Option:

- **status** -- Check if the running configuration differs from the statup configuration.**(p. 384)**

sampling-polling

- show sflow *< 1 to 3 >* sampling-polling

© 2007 Hewlett-Packard Development Company, L.P.

```
Displays information about sampling and polling.
```

Next Available Option:
- **port-list** -- Displays information about sampling and polling. ([ethernet] PORT-LIST) **(p. 371)**

sec-model

- show snmpv3 access-rights *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* sec-model

```
Set security model.
```

Next Available Options:
- **ver1-2c** < ver1 | ver2c > -- Configure SNMPv3 User entry.**(p. 388)**
- **ver3** -- SNMP version 3 security model.**(p. 388)**

- show snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* user *USER* sec-model *< ver1 | ver2c | ver3 >*

```
Show a specific security model.
```

Supported Values:
- **ver1** -- SNMP version 1 security model.
- **ver2c** -- SNMP version v2c security model.
- **ver3** -- SNMP version 3 security model.

sequence-number

- show ip ospf external-link-state sequence-number *INTEGER*

```
Show LSAs with the specified sequence number only.
```

- show ip ospf link-state sequence-number *INTEGER*

```
Show LSAs with the specified sequence number only.
```

session-counters

- show port-access authenticator session-counters

```
Show 802.1x current (or last if no current sessions open) sessions counters.
```

sessions

- show accounting sessions

```
Usage: show accounting sessions

Description: Show accounting data for all active sessions.
```

sflow

- show sflow

```
Usage: show sflow <agent | destination | all |
                   sampling-polling [ethernet] PORT-LIST>

Description: Display information regarding the configuration,
             sampling, and polling with respect to 'sflow'.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:
- **agent** -- Displays read-only switch agent information: The agent address is normally the ip address of the first vlan configured.**(p. 334)**
- **receiver-index** < 1 to 3 > -- Select one of the three possible sFlow receiver tables. (NUMBER) **(p. 375)**

slave_time

- show cpu slot *SLOT-ID-RANGE < 1 to 90 >*

```
Time (seconds) over which to average CPU utilization.
```

Range: < 1 to 90 >

slot

- show cpu slot *SLOT-ID-RANGE*

```
Display module CPU statistics.
```

Next Available Option:
- **slave_time** < 1 to 90 > -- Time (seconds) over which to average CPU utilization. (NUMBER) **(p. 380)**

- show power-management brief slot *SLOT-ID-RANGE*

```
Usage: show power-management brief

Description: Show summary of power status.
```

snmp-server

- show snmp-server

```
Usage: show snmp-server [COMMUNITY-STR]

Description: Display information on all SNMP communities, trap receivers and
             Snmp response/trap source-ip policy configured on the switch. If
             'COMMUNITY-STR' is specified, only information for that community
             is displayed.
```

Next Available Option:
- **community** -- Specify SNMP community to which to restrict the output. (ASCII-STR) **(p. 340)**

snmpv3

- show snmpv3

```
Show configuration of SNMPv3 features.
```

Next Available Options:
- **access-rights** -- Show information about access rights. **(p. 333)**
- **community** -- Show SNMPv3 Community table. **(p. 340)**
- **enable** -- Show SNMPv3 status. **(p. 347)**
- **engineid** -- Show switch's SNMP engineId. **(p. 348)**
- **group** -- Show SNMPv3 User to Group mappings. **(p. 351)**

© 2007 Hewlett-Packard Development Company, L.P.

- **notify** -- Show SNMPv3 notification table. **(p. 368)**
- **only** -- Show SNMP message reception policy. **(p. 369)**
- **params** -- Show SNMPv3 Target Parameters table. **(p. 370)**
- **restricted-access** -- Show SNMPv1 and SNMPv2c access properties. **(p. 376)**
- **targetaddress** -- Show SNMPv3 Target Address table. **(p. 384)**
- **user** -- Show SNMPv3 users. **(p. 388)**
- **view** -- Show views. **(p. 389)**

sntp

- show sntp

```
Usage: show sntp

Description: Show configured time protocol and servers.
```

source-port

- show filter source-port

```
Usage: show filter source-port

Description: Show a table of source-port filter names
             with the associated source ports and actions
```

spanning-tree

- show spanning-tree

```
Usage: show spanning-tree [[ethernet] PORT-LIST] [config|detail]
       show spanning-tree [[ethernet] PORT-LIST] instance <ist|INSTANCE-ID>
       [detail]
       show spanning-tree [mst-config] | [config instance <ist|INSTANCE-ID>]

Description: Show spanning tree information.
             When executed without parameters, the command shows spanning
             tree status information. If PORT-LIST is specified, the
             command shows spanning tree status information only for the
             ports listed.
             If the 'detail' keyword is specified, extended port, cost,
             and BPDU information is shown.
             If MSTP is on, the 'instance' command can be issued to specify
             a particular instance to be displayed for the 'detail' keyword.
             If the 'config' keyword is specified the spanning tree
             configuration information is shown.
             The second form of the command can be used to show MSTP
             specific information. Use the 'show spanning-tree ?'
             command to see all available parameters with description.
```

Next Available Options:

- **port-list** -- Limit the port information printed to the set of the specified ports. ([ethernet] PORT-LIST) **(p. 371)**
- **detail** -- Show spanning tree extended details Port, Bridge, Rx, and Tx report.**(p. 345)**
- **config** -- Show spanning tree configuration information.**(p. 341)**
- **instance** -- Show spanning tree instance status information.**(p. 354)**
- **mst-config** -- Show multiple spanning tree region configuration.**(p. 367)**
- **pending** -- Show spanning tree pending configuration**(p. 370)**

© 2007 Hewlett-Packard Development Company, L.P.

- **traps** -- Show spanning tree trap information.**(p. 386)**
- **bpdu-protection** -- Show spanning tree BPDU protection status information.**(p. 338)**

ssh

- show ip ssh

```
Usage: show ip ssh

Description: Show both current SSH configuration and the status of active
             connections.
```

stack

- show stack

```
Usage: show stack [candidates|view|all]

Description: Show the stack status of this switch. The 'candidate' and
             'view' commands are available on the stack commander only.

    o candidates - show the list of devices that are stack candidates.

    o view - show the list of devices that are stack members.

    o all - show information about all the stacks available on the LAN.
```

Next Available Options:

- **candidates** -- Show the list of devices that are stack candidates.**(p. 339)**
- **view** -- Show the list of devices that are stack members.**(p. 389)**
- **all** -- Show information about all the stacks available on the LAN.**(p. 334)**

static

- show ip pim rp-set static

```
Show statically configured RP-Set information.
```

static-mac

- show static-mac

```
Usage: show static-mac

Description: Show the locked-down MAC addresses in all vlans.
             The list is sorted by VLAN, then MAC address.
```

statistics

- show arp-protect statistics <VLAN-ID-RANGE>

```
Show statistics about forwarded ARP packets, dropped ARP packets, MAC
validation failure, and IP validation failure. You can enter a range of
VLAN-IDs, for example, 1-20.
```

- show link-keepalive statistics

© 2007 Hewlett-Packard Development Company, L.P.

```
show detailed statistics for all link-keepalive enabled ports.
```

- show port-access authenticator statistics

```
Show authentication sessions statistics for 802.1x authenticator.
```

- show port-access supplicant statistics

```
Show authentication sessions statistics for 802.1x supplicant.
```

- show rmon statistics *[ETHERNET] PORT-LIST*

```
Usage: show rmon statistics PORT-LIST

Description: Show RMON statistics for the ports.
```

- show tech statistics

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

- show vrrp statistics

```
Usage: show vrrp statistics

Description: Show VRRP statistics information for the device.
```

Next Available Option:

- **global** -- Show global VRRP configuration information. **(p. 350)**

- show vrrp vlan *VLAN-ID* statistics

```
Show VRRP statistics information for the VLAN.
```

- show vrrp vlan *VLAN-ID* vrid *< 1 to 255 >* statistics

```
Show virtual router statistics information.
```

stats

- show dhcp-snooping stats

```
Display DHCP snooping events.
```

- show lldp stats

```
Usage: show lldp stats [[ethernet] PORT-LIST]

Description: Show LLDP statistics.
   o [ethernet] PORT-LIST - Show statistics for the specified ports .
```

Next Available Option:

- **port-list** -- Specify the port or list of ports. ([ethernet] PORT-LIST) **(p. 371)**

© 2007 Hewlett-Packard Development Company, L.P.

status

- show config status

```
Check if the running configuration differs from the statup configuration.
```

- show ip ospf external-link-state status

```
The keyword is optional and can be omitted.
```

- show ip ospf link-state status

```
The keyword is optional and can be omitted.
```

- show running-config status

```
Check if the running configuration differs from the statup configuration.
```

SUB-TREE

- show snmpv3 view *VIEW-NAME SUB-TREE*

```
Set the OID of the tree.
```

supplicant

- show port-access supplicant

```
Usage: show port-access supplicant [statistics]

Description: Show 802.1x (Port Based Network Access) supplicant
             current status and configuration.
```

Next Available Options:

- **ports** -- Show information for specified ports only. ([ethernet] PORT-LIST) **(p. 373)**
- **statistics** -- Show authentication sessions statistics for 802.1x supplicant.**(p. 382)**

system-information

- show system-information

```
Usage: show system-information

Description: Show global configured and operational system parameters.
```

tacacs

- show tacacs

```
Usage: show tacacs

Description: Show TACACS status and statistics.
```

targetaddress

- show snmpv3 targetaddress

```
Show SNMPv3 Target Address table.
```

Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **TARGETADDR-NAME** -- Show a specifc target address entry. (ASCII-STR) **(p. 385)**

TARGETADDR-NAME

- show snmpv3 targetaddress *TARGETADDR-NAME*

```
Show a specifc target address entry.
```

tcp-udp-port-priority

- show qos tcp-udp-port-priority

```
Usage: show qos tcp-udp-port-priority

Description: Show TCP/UDP port priorities.
```

tech

- show tech

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Shows switch operating and running configuration details.
```

Next Available Options:

- **all** -- Shows switch operating and running configuration details, including image stamp, event log listing, boot history, port settings and status, IP routes, GVRP support, and load balancing (trunk and LACP).**(p. 334)**
- **buffers** -- Displays buffer contents. **(p. 339)**
- **instrumentation** -- Shows a variety of information including the status of IGMP and routing. **(p. 356)**
- **mesh** -- Shows meshing information, including ports, the port state, the adjacent switch, and the peer port. **(p. 365)**
- **route** -- Shows IP routing information.**(p. 377)**
- **statistics** -- Shows port transitions for each slot in the switch. **(p. 382)**
- **transceivers** -- Allows you to remotely identify transceiver type and revision number without having to physically remove an installed transceiver from its slot. Displays real-time status information about all installed transceivers, including non-operational transceivers.**(p. 386)**

telnet

- show telnet

```
Usage: show telnet

Description: Show active incoming and outgoing sessions.
```

temperature

- show temperature

```
Usage: show temperature

Description: Show systems temperatures and settings.
```

© 2007 Hewlett-Packard Development Company, L.P.

terminal

- show terminal

```
Usage: show terminal

Description: Show logical window dimensions.
```

throttled-hosts

- show connection-rate-filter throttled-hosts

```
Show throttled IP addresses.
```

time

- show cpu *< 1 to 300 >*

```
Time (seconds) over which to average CPU utilization.
```

Range: < 1 to 300 >

- show time

```
Usage: show time

Description: Show current date and time.
```

timep

- show timep

```
Usage: show timep

Description: Show configured time protocol and servers.
```

transceivers

- show tech transceivers

```
Usage: show tech [all|buffers|mesh|route|statistics]

Description: Display output of a predefined command sequence used by
             technical support.
```

traps

- show ip ospf traps

```
Usage: show ip ospf traps

Description: Show OSPF traps enabled on the device.
```

- show spanning-tree traps

```
Show spanning tree trap information.
```

trunks

- show trunks

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: show trunks [[ethernet] PORT-LIST]

Description: Show a list of ports and the trunks to which they belong.
             If a PORT-LIST is supplied the command shows only the ports
             specified.
```

Next Available Option:

- **port-list** -- Show the trunk information only for the ports specified. ([ethernet] PORT-LIST) **(p. 371)**

type

- show ip ospf link-state type *< router | network | summary | ... >*

```
Show LSAs of the specified type only.
```

Supported Values:

- **router** -- Show router links only.
- **network** -- Show network links only.
- **summary** -- Show summary links only.
- **as-summary** -- Show Autonomous System summary links only.
- **external** -- Show Autonomous System external links only.
- **multicast** -- Show multicast links only.
- **nssa** -- Show NSSA external links only.

- show ip route *< static | connected | rip | ... >*

```
Specify type of routes to display.
```

Supported Values:

- **static** -- Show static routes only.
- **connected** -- Show the switch's interface routes only.
- **rip** -- Show RIP routes only.
- **ospf** -- Show OSPF routes only.

type-of-service

- show qos type-of-service

```
Usage: show qos type-of-service

Description: Show QoS priorities based on IP Type-of-Service.
```

uninstalled

- show licenses uninstalled

```
Display verification key for features which have been uninstalled.
```

uptime

- show uptime

```
Usage: show uptime

Description: Displays elapsed time since last boot.
```

© 2007 Hewlett-Packard Development Company, L.P.

user

- show snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* user *USER*

  Show a specific user.

  Next Available Option:
  - **sec-model** < ver1 | ver2c | ver3 > -- Show a specific security model. **(p. 379)**

- show snmpv3 user

  Show SNMPv3 users.

  Next Available Option:
  - **USER-NAME** -- Show a specific user. (ASCII-STR) **(p. 388)**

USER-NAME

- show snmpv3 user *USER-NAME*

  Show a specific user.

ver1-2c

- show snmpv3 access-rights *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* sec-model *< ver1 | ver2c >*

  Configure SNMPv3 User entry.

  Supported Values:
  - **ver1** -- SNMP version 1 security model.
  - **ver2c** -- SNMP version 2c security model.

ver3

- show snmpv3 access-rights *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* sec-model ver3

  SNMP version 3 security model.

  Next Available Option:
  - **ver3** < noauth | auth | priv > -- Set security level. **(p. 388)**

- show snmpv3 access-rights *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* sec-model ver3 *< noauth | auth | priv >*

  Set security level.

  Supported Values:
  - **noauth** -- no authentication (and no privacy)
  - **auth** -- authentication (no privacy)
  - **priv** -- authentication and privacy

version

- show version

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: show version

Description: Show software version.
```

view

- show snmpv3 view

```
Show views.
```

Next Available Option:
- **VIEW-NAME** -- Set view name. (ASCII-STR) **(p. 389)**

- show stack view

```
Show the list of devices that are stack members.
```

VIEW-NAME

- show snmpv3 view *VIEW-NAME*

```
Set view name.
```

Next Available Option:
- **SUB-TREE** -- Set the OID of the tree. (ASCII-STR) **(p. 384)**

virtual-link

- show ip ospf virtual-link

```
Usage: show ip ospf virtual-link [IP-ADDR] [area OSPF-AREA-ID]

Description: Show status of all OSPF virtual links configured.
             The 'IP-ADDR' can be specified to display detailed
             information for a particular virtual neighbor. If
             the area is specified only virtual links of the
             area are shown.
```

Next Available Options:
- **vlink-ip** -- Router ID of the link destination for which to show detailed information. (IP-ADDR) **(p. 391)**
- **area** -- Specify area of the virtual links to show. (OSPF-AREA-ID) **(p. 334)**

virtual-neighbor

- show ip ospf virtual-neighbor

```
Usage: show ip ospf virtual-neighbor [IP-ADDR]
                                     [area OSPF-AREA-ID]

Description: Show all virtual neighbors of the device.
             The 'IP-ADDR' can be specified to display detailed
             information for a particular virtual neighbor. If
             the area is specified only virtual neighbors belonging
             to the area are shown.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:
- **vneighbor-ip** -- Router ID of the virtual neighbor for which to show detailed information. (IP-ADDR) **(p. 391)**
- **area** -- Specify area of the virtual neighbors to show. (OSPF-AREA-ID) **(p. 334)**

vlan

- show access-list vlan *VLAN-ID*

  ```
  Show ACLs applied to the specified VLAN.
  ```

- show arp vlan *VLAN-ID*

  ```
  Specify VLAN for which to show ARP entries.
  ```

- show ip helper-address vlan *VLAN-ID*

  ```
  Specify a vlan for which to show server addresses.
  ```

- show ip forward-protocol vlan *VLAN-ID*

  ```
  Specify a vlan for which to show server addresses.
  ```

- show ip igmp *VLAN-ID*

  ```
  Show IGMP operational information for the VLAN specified.
  ```

  Next Available Option:
  - **config** -- Show IGMP configuration information for the VLAN specified.**(p. 341)**

- show ip ospf interface vlan *VLAN-ID*

  ```
  Specify VLAN of the interface for which to show detailed information.
  ```

- show ip rip interface vlan *VLAN-ID*

  ```
  Specify VLAN of the interface for which to show detailed information.
  ```

- show mac-address vlan *VLAN-ID*

  ```
  Show MAC addresses learned on the specified VLAN.
  ```

- show port-access authenticator vlan

  ```
  Show authorized and unauthorized vlans for 802.1x authenticator.
  ```

- show vlans *VLAN-ID*

  ```
  Show detailed VLAN information for the VLAN with the ID supplied.
  ```

- show vrrp vlan

  ```
  Show VRRP information for a VLAN.
  ```

  Next Available Option:
  - **VLAN-ID** -- Specify VLAN for which to display VRRP information. (VLAN-ID) **(p. 391)**

© 2007 Hewlett-Packard Development Company, L.P.

VLAN-ID

- show ip mroute interface *VLAN-ID*

```
Specify the VLAN ID of the IP multicast routing interface to show.
```

- show ip pim interface *VLAN-ID*

```
Specify the VLAN ID of the PIM interface to show.
```

- show vrrp vlan *VLAN-ID*

```
Specify VLAN for which to display VRRP information.
```

Next Available Options:

- **config** -- Show VRRP configuration information for the VLAN. **(p. 341)**
- **statistics** -- Show VRRP statistics information for the VLAN. **(p. 382)**
- **vrid** -- Show information for a virtual router. **(p. 392)**

vlan-priority

- show qos vlan-priority

```
Usage: show qos vlan-priority

Description: Show the VLAN-based priority table.
```

vlans

- show igmp-proxy vlans

```
Show all the VLANs currently associated with IGMP proxy domains.
```

- show vlans

```
Usage: show vlans [VLAN-ID|ports [ethernet] PORT-LIST]

Description: Show status information for all VLANs.
             If a 'VLAN-ID' is specified, shows the ports that are currently
             members of the VLAN identified by the 'VLAN-ID'.
             If a 'PORT-LIST' is specified, shows all the VLANs of which
             at least one port in the 'PORT-LIST' is a member.
```

Next Available Options:

- **vlan** -- Show detailed VLAN information for the VLAN with the ID supplied. (VLAN-ID) **(p. 390)**
- **ports** -- Show VLANs that have at least one port from the 'PORT-LIST' as a member. ([ethernet] PORT-LIST) **(p. 373)**

vlink-ip

- show ip ospf virtual-link *IP-ADDR*

```
Router ID of the link destination for which to show detailed information.
```

vneighbor-ip

- show ip ospf virtual-neighbor *IP-ADDR*

© 2007 Hewlett-Packard Development Company, L.P.

```
Router ID of the virtual neighbor for which to show detailed information.
```

vrid

- show vrrp vlan *VLAN-ID* vrid

```
Show information for a virtual router.
```

Next Available Option:
- **VRID** < 1 to 255 > -- Specify virtual router for which to display information. **(p. 392)**

VRID

- show vrrp vlan *VLAN-ID* vrid *< 1 to 255 >*

```
Specify virtual router for which to display information.
```

Range: < 1 to 255 >

Next Available Options:
- **config** -- Show virtual router configuration information. **(p. 341)**
- **statistics** -- Show virtual router statistics information. **(p. 382)**

vrrp

- show vrrp

```
Usage: show vrrp [...]

Description: Show VRRP configuration and statistics information.
```

Next Available Options:
- **config** -- Show VRRP configuration information for the device**(p. 341)**
- **statistics** -- Show VRRP statistics information for the device**(p. 382)**
- **vlan** -- Show VRRP information for a VLAN. **(p. 390)**

web-based

- show port-access web-based

```
Usage: show port-access [PORT-LIST] web-based
                        [<config [auth-server|web-server|detail]>|clients]
       show port-access web-based [PORT-LIST]
                        [<config [auth-server|web-server|detail]>|clients]
       show port-access web-based config [PORT-LIST]
                                 [auth-server|web-server|detail]

Description: Show Web Authentication statistics and configuration. If
             PORT-LIST parameter has been specified then information only
             for the specified ports is shown.
             If 'config' keyword has been specified then the configuration
             of Web Authentication is shown.
             If 'auth-server' keyword has been specified then the
             authentication server-related configuration items are shown.
             If 'web-server' keyword has been specified then the web
```

© 2007 Hewlett-Packard Development Company, L.P.

```
server-related configuration items are shown.
If PORT-LIST and 'detail' keyword has been specified then the
detailed configuration of Web Authentication for the specified
ports is shown.
If 'clients' keyword has been specified then the current client
session statistics is shown.
```

Next Available Options:

- -- Specify ports for which Web Authentication information will be shown. ([ethernet] PORT-LIST) (p. 331)
- **config** -- Show the current configuration of Web Authentication.(p. 341)
- **clients** -- Show the current client session statistics.(p. 340)

- show port-access *[ETHERNET] PORT-LIST* web-based

```
Usage: show port-access [PORT-LIST] web-based
                        [<config [auth-server|web-server|detail]>|clients]
       show port-access web-based [PORT-LIST]
                        [<config [auth-server|web-server|detail]>|clients]
       show port-access web-based config [PORT-LIST]
                                 [auth-server|web-server|detail]

Description: Show Web Authentication statistics and configuration. If
             PORT-LIST parameter has been specified then information only
             for the specified ports is shown.
             If 'config' keyword has been specified then the configuration
             of Web Authentication is shown.
             If 'auth-server' keyword has been specified then the
             authentication server-related configuration items are shown.
             If 'web-server' keyword has been specified then the web
             server-related configuration items are shown.
             If PORT-LIST and 'detail' keyword has been specified then the
             detailed configuration of Web Authentication for the specified
             ports is shown.
             If 'clients' keyword has been specified then the current client
             session statistics is shown.
```

Next Available Options:

- **config** -- Show the current configuration of Web Authentication.(p. 341)
- **clients** -- Show the current client session statistics.(p. 340)

web-server

- show port-access web-based *[ETHERNET] PORT-LIST* config web-server

```
Show the web server-related configuration items.
```

- show port-access web-based config *[ETHERNET] PORT-LIST* web-server

```
Show the web server-related configuration items.
```

- show port-access web-based config web-server

```
Show the web server-related configuration items.
```

- show port-access *[ETHERNET] PORT-LIST* web-based config web-server

© 2007 Hewlett-Packard Development Company, L.P.

```
Show the web server-related configuration items.
```

© 2007 Hewlett-Packard Development Company, L.P.

snmp-server

OVERVIEW

Category:	SNMP
Primary context:	config
Related Commands	**show snmpv3 (page 380)**

```
Usage: snmp-server [contact ASCII-STR]
                   [location ASCII-STR]
       [no] snmp-server community ASCII-STR
                   [manager|operator] [restricted|unrestricted]
       [no] snmp-server host IP-ADDR COMMUNITY-STR
                   [none|debug|all|not-info|critical]
       [no] snmp-server enable
       [no] snmp-server enable traps authentication
       [no] snmp-server enable traps link-change <PORT-LIST>
       [no] snmp-server response-source [IP-ADDR|dst-ip-of-request|
                                         loopback<0-7>]
       [no] snmp-server trap-source [IP-ADDR|loopback<0-7>]

Description: Configure the device SNMP server.
   The first version of the command specifies system contact and
   location.

   The second version may be used to add, edit or delete a SNMP community.
   Use 'snmp-server community help' to get a detailed on the command.

   The third version defines SNMP traps and their receivers.
   The command configures which network management stations
   will receive SNMP event log messages from the switch and
   the types of events for which the switch will send these
   messages. In all cases, the switch will send all messages
   resulting from thresholds, to the network management
   station that explicitly set each threshold. The levels
   specified on this screen correspond only to the traps set
   for event log messages, not to those set for thresholds.

   You can specify up to 10 trap receivers (network management
   stations).

   The fourth version of the command enables or disables SNMPv1/v2.

   The fifth version enables or disables authentication traps to be sent
   when a management station attempts an unauthorized access.

   The sixth version enables or disables linkup/linkdown traps to be sent.
   on a per-port basis by accepting a port list. By default, linkup/linkdown
   traps are enabled for all ports. Ports are disabled by using the command
   in the [no] form.

   The seventh version of the command configures the policy for the source-ip
   address of the snmp response pdu. Use 'snmp-server response-source help'
   to get a detailed on the command.

   The last version of the command configures the policy for the source-ip
```

© 2007 Hewlett-Packard Development Company, L.P.

```
   address of the snmp trap pdu. Use 'snmp-server trap-source help' to get
   a detailed on the command.

Parameters:

    o contact ASCII-STR - Up to 48 characters. Name of the switch
      administrator.

    o location ASCII-STR - Up to 48 characters. Description of the
      switch location.

    o community ASCII-STR - Enter up to 32 characters to name an SNMP
      community.

    o <manager|operator> - manager - the community can access all MIB
      objects; operator (default) - the community can access all except
      the CONFIG MIB.

    o <restricted|unrestricted> - unrestricted - any MIB variable that
      has read/write access can be set; restricted (default) - MIB
      variables cannot be set, only read.

    o IP-ADDR - Address of the network management station.

    o [none|all|not-info|critical|debug] - The level of Switch
      events that will generate a Trap to be sent: none - send no log
      message; all - send all log messages; not-info - send each log
      message that is not informational-only; critical - send
      critical-level log messages; debug (reserved for Internal use).

    o [IP-ADDR|loopback<0-7>|dst-ip-of-request] - Policy type used to
      fill the source-ip address field of the snmp response/trap pdu:
      IP-ADDR - This ip address will be used while sending the
      snmp response/trap pdu; loopback<0-7> - lexicographically min.
      configured ip address on specified loopback interface will be
      used while sending the response; dst-ip-of-request - destination
      ip address passed in the request pdu will be send as the source-ip
      address in the response pdu.
```

Caution

Downloading and booting from the M.08.89 or greater software version for the first time enables SNMP access to the authentication configuration MIB (the default action). If SNMPv3 and other security safeguards are not in place, the switch's authentication configuration MIB is exposed to unprotected SNMP access. See the following Note.

NOTES

SNMP Access to the Switch's Authentication Configuration MIB

A management station running an SNMP networked device management application such as ProCurve Manager Plus (PCM+) or HP OpenView can access the switch's management information base (MIB) for read access to the switch's status and read/write access to the switch's configuration. In earlier software versions, SNMP access to the switch's authentication configuration (hpSwitchAuth) MIB was not allowed. However, beginning with software release M.08.89, the switch's default configuration allows SNMP access to security settings in hpSwitchAuth. If SNMP access to the hpSwitchAuth MIB is considered a security risk in your

© 2007 Hewlett-Packard Development Company, L.P.

network, then you should implement the following security precautions when downloading and booting from software release M.08.89 or greater:

1. If SNMP access to the authentication configuration (hpSwitchAuth) MIB described above is not desirable for your network, then immediately after downloading and booting from the M.08.89 or greater software for the first time, use the following command to disable this feature:

snmp-server mib hpswitchauthmib excluded

2. If you choose to leave the authentication configuration MIB accessible, then you should do the following to help ensure that unauthorized workstations cannot use SNMP tools to access the MIB:

- Configure SNMP version 3 management and access security on the switch.

- Disable SNMP version 2c on the switch.

COMMAND STRUCTURE

- [no] snmp-server **community** -- Add/delete SNMP community (ASCII-STR) **(p. 398)**
  - **view < Operator | Manager >** -- Add/delete SNMP community **(p. 403)**
  - **write-access < Restricted | Unrestricted | | ... >** -- Add/delete SNMP community **(p. 403)**
- snmp-server **contact** -- Name of the switch administrator. (ASCII-STR) **(p. 399)**
- [no] snmp-server **enable** -- Enable/Disable SNMPv1/v2 **(p. 399)**
  - **traps** -- Enable/disable authentication traps to be sent when a management station attempts an unauthorized access **(p. 402)**
    - **authentication** -- Authentication SNMP traps. **(p. 398)**
    - **link-change** -- Link-status SNMP traps. ([ethernet] PORT-LIST) **(p. 401)**
- [no] snmp-server **host** -- Define SNMP traps and their receivers **(p. 399)**
  - **address** -- IP address of SNMP notification host. (IP-ADDR) **(p. 398)**
  - **community** -- Name of the SNMP community (up to 32 characters). (ASCII-STR) **(p. 398)**
  - **events < None | Debug | All | ... >** -- **(p. 399)**
- snmp-server **location** -- Description of the switch location. (ASCII-STR) **(p. 401)**
- snmp-server **mib** -- Enable/Disable SNMP support for the hpSwitchAuthentication MIB **(p. 401)**
  - **hpSwitchAuthMIB** -- Enable/Disable SNMP support for the hpSwitchAuthentication MIB **(p. 400)**
    - **excluded** -- Disables SNMP support for the hpSwitchAuthentication MIB. **(p. 399)**
    - **included** -- Enables SNMP support for the hpSwitchAuthentication MIB. **(p. 400)**
- [no] snmp-server **response-source** -- Specify the source ip-address policy for the response pdu **(p. 401)**
  - **dst-ip-of-request** -- Destination Ip address of the snmp request pdu will be used as the source ip address in the snmp response pdu. **(p. 399)**
  - **ip-addr** -- IP Address for the source ip address field in the snmp response pdu. (IP-ADDR) **(p. 401)**
  - **loopback < 0 to 7 >** -- For the specified loopback interface, lexicographically minimum configured ip address will be used as the source ip address in the snmp response pdu. **(p. 401)**
- [no] snmp-server **trap-source** -- Specify the source ip-address policy for the trap pdu **(p. 402)**
  - **ip-addr** -- IP Address for the source ip address field in the trap pdu. (IP-ADDR) **(p. 401)**
  - **loopback < 0 to 7 >** -- For the specified loopback interface, lexicographically minimum configured ip address will be used as the source ip address in the trap pdu. **(p. 401)**

© 2007 Hewlett-Packard Development Company, L.P.

EXAMPLES

Example: snmp-server community

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)

```
ProCurve(config)# snmp-server community red-team manager unrestricted
ProCurve(config)# snmp-server community blue-team operator restricted
```

COMMAND DETAILS

address (p. 398)	excluded (p. 399)	loopback (p. 401)
authentication (p. 398)	host (p. 399)	mib (p. 401)
community (p. 398)	hpSwitchAuthMIB (p. 400)	response-source (p. 401)
contact (p. 399)	included (p. 400)	traps (p. 402)
dst-ip-of-request (p. 399)	ip-addr (p. 401)	trap-source (p. 402)
enable (p. 399)	link-change (p. 401)	view (p. 403)
events (p. 399)	location (p. 401)	write-access (p. 403)

address

- snmp-server host *IP-ADDR*

```
IP address of SNMP notification host.
```

authentication

- [no] snmp-server enable traps authentication

```
Authentication SNMP traps.
```

community

- [no] snmp-server community *COMMUNITY*

```
Usage: [no] snmp-server community ASCII-STR
                    [manager|operator] [restricted|unrestricted]

Description: Add/delete SNMP community.

Parameters:

    o community ASCII-STR - Enter up to 32 characters to name an SNMP
      community.

    o <manager|operator> - manager - the community can access all MIB
      objects; operator (default) - the community can access all except
      the CONFIG MIB.

    o <restricted|unrestricted> - unrestricted - any MIB variable that
```

© 2007 Hewlett-Packard Development Company, L.P.

```
has read/write access can be set; restricted (default) - MIB
variables cannot be set, only read.
```

Next Available Options:
- **view** < Operator | Manager > -- Add/delete SNMP community**(p. 403)**
- **write-access** < Restricted | Unrestricted | | ... > -- Add/delete SNMP community**(p. 403)**

- snmp-server host *COMMUNITY*

```
Name of the SNMP community (up to 32 characters).
```

contact

- snmp-server contact *CONTACT*

```
Name of the switch administrator.
```

dst-ip-of-request

- snmp-server response-source dst-ip-of-request

```
Destination Ip address of the snmp request pdu will be used as the
source ip address in the snmp response pdu.
```

enable

- [no] snmp-server enable

```
Usage: [no] snmp-server enable

Description:Enable/Disable SNMPv1/v2.
```

Next Available Option:
- **traps** -- Enable/disable authentication traps to be sent when a management station attempts an unauthorized access**(p. 402)**

events

- snmp-server host *< None | Debug | All | ... >*

Supported Values:
- **None** -- Send no log messages.
- **Debug** -- Send debug traps (for Internal use).
- **All** -- Send all log messages
- **Not-INFO** -- Send all but informational-only messages.
- **Critical** -- Send critical-level log messages.

excluded

- snmp-server mib hpSwitchAuthMIB excluded

```
Disables SNMP support for the hpSwitchAuthentication MIB.
```

host

- [no] snmp-server host

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] snmp-server host IP-ADDR COMMUNITY-STR
                  [none|debug|all|not-info|critical]

Description: Define SNMP traps and their receivers.
             This command configures which network management stations
             will receive SNMP event log messages from the switch and
             the types of events for which the switch will send these
             messages. In all cases, the switch will send all messages
             resulting from thresholds, to the network management
             station that explicitly set each threshold. The levels
             specified on this screen correspond only to the traps set
             for event log messages, not to those set for thresholds.

             You can specify up to 10 trap receivers (network management
             stations).

Parameters:

    o COMMUNITY-STR - SNMP community string.

    o IP-ADDR - IP address of SNMP notification host.

    o [none|all|not-info|critical|debug] - The level of Switch
      events that will generate a trap to be sent: none - send no log
      message; all - send all log messages; not-info - send each log
      message that is not informational-only; critical - send
      critical-level log messages; debug (reserved for Internal use).
```

Next Available Options:

- **address** -- IP address of SNMP notification host. (IP-ADDR) **(p. 398)**
- **community** -- Name of the SNMP community (up to 32 characters). (ASCII-STR) **(p. 398)**
- **events** < None | Debug | All | ... > -- **(p. 399)**

hpSwitchAuthMIB

- snmp-server mib hpSwitchAuthMIB

```
Usage: snmp-server mib hpSwitchAuthMIB <excluded|included>

Description: Enable/Disable SNMP support for the hpSwitchAuthentication MIB.
             When the MIB access is enabled, Manager read/write access
             to the MIB is permitted. Operator read/write access to the MIB
             is always denied. For security reasons, network administrators
             are encouraged to disable SNMPV2c before using the MIB.
```

Next Available Options:

- **included** -- Enables SNMP support for the hpSwitchAuthentication MIB.**(p. 400)**
- **excluded** -- Disables SNMP support for the hpSwitchAuthentication MIB.**(p. 399)**

included

- snmp-server mib hpSwitchAuthMIB included

```
Enables SNMP support for the hpSwitchAuthentication MIB.
```

© 2007 Hewlett-Packard Development Company, L.P.

ip-addr

- snmp-server response-source *IP-ADDR*

```
IP Address for the source ip address field in the snmp response pdu.
```

- snmp-server trap-source *IP-ADDR*

```
IP Address for the source ip address field in the trap pdu.
```

link-change

- [no] snmp-server enable traps link-change *[ETHERNET] PORT-LIST*

```
Link-status SNMP traps.
```

location

- snmp-server location *LOCATION*

```
Description of the switch location.
```

loopback

- snmp-server response-source loopback *< 0 to 7 >*

```
For the specified loopback interface, lexicographically minimum
configured ip address will be used as the source ip address in
the snmp response pdu.
```

Range: < 0 to 7 >

- snmp-server trap-source loopback *< 0 to 7 >*

```
For the specified loopback interface, lexicographically minimum
configured ip address will be used as the source ip address in
the trap pdu.
```

Range: < 0 to 7 >

mib

- snmp-server mib

```
Usage: snmp-server mib hpSwitchAuthMIB <excluded|included>

Description: Enable/Disable SNMP support for the hpSwitchAuthentication MIB.
             When the MIB access is enabled, Manager read/write access
             to the MIB is permitted. Operator read/write access to the MIB
             is always denied. For security reasons, network administrators
             are encouraged to disable SNMPV2c before using the MIB.
```

Next Available Option:

- **hpSwitchAuthMIB** -- Enable/Disable SNMP support for the hpSwitchAuthentication MIB**(p. 400)**

response-source

- [no] snmp-server response-source

```
Usage: [no] snmp-server response-source [IP-ADDR|dst-ip-of-request|
                                         loopback<0-7>]
```

© 2007 Hewlett-Packard Development Company, L.P.

```
Description: Specify the source ip-address policy for the response pdu.
             By default snmp response pdu will contain the ip address of
             the active interface on which response will be sent. The default
             behavior is in compliance to rfc-1517.
             The no form of the command will revert to default behavior.

IP-ADDR            -- ip-address specified will be used as the source ip
                      address in the snmp response pdu.
dst-ip-of-request  -- Destination ip of the snmp request will be used as
                      the source ip address in the snmp response pdu.
loopback 0-7       -- lexicographically minimum configured ip address on the
                      specified interface will be used as the source ip
                      address in the snmp response pdu.
```

Next Available Options:

- **ip-addr** -- IP Address for the source ip address field in the snmp response pdu. (IP-ADDR) **(p. 401)**
- **dst-ip-of-request** -- Destination Ip address of the snmp request pdu will be used as the source ip address in the snmp response pdu.**(p. 399)**
- **loopback** < 0 to 7 > -- For the specified loopback interface, lexicographically minimum configured ip address will be used as the source ip address in the snmp response pdu.**(p. 401)**

traps

- [no] snmp-server enable traps

```
Usage: [no] snmp-server enable traps authentication
       [no] snmp-server enable traps link-change <PORT-LIST>

Description: Enable/disable authentication traps to be sent when a
             management station attempts an unauthorized access.
```

Next Available Options:

- **link-change** -- Link-status SNMP traps. ([ethernet] PORT-LIST) **(p. 401)**
- **authentication** -- Authentication SNMP traps.**(p. 398)**

trap-source

- [no] snmp-server trap-source

```
Usage: [no] snmp-server trap-source [IP-ADDR|loopback<0-7>]

Description: Specify the source ip-address policy for the trap pdu.
             By default snmp trap pdu will contain the ip address of
             the active interface on which trap will be sent. The default
             behavior is in compliance to rfc-1517.
             The no form of the command will revert to default behavior.

IP-ADDR            -- ip-address specified will be used as the source ip
                      address in the generated trap.
loopback 0-7       -- lexicographically minimum configured ip address on the
                      specified interface will be used as the source ip
                      address in the generated trap pdu.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **ip-addr** -- IP Address for the source ip address field in the trap pdu. (IP-ADDR) **(p. 401)**
- **loopback** < 0 to 7 > -- For the specified loopback interface, lexicographically minimum configured ip address will be used as the source ip address in the trap pdu.**(p. 401)**

view

- [no] snmp-server community *COMMUNITY* < *Operator* | *Manager* >

```
Usage: [no] snmp-server community ASCII-STR
                    [manager|operator] [restricted|unrestricted]

Description: Add/delete SNMP community.

Parameters:

    o community ASCII-STR - Enter up to 32 characters to name an SNMP
      community.

    o <manager|operator> - manager - the community can access all MIB
      objects; operator (default) - the community can access all except
      the CONFIG MIB.

    o <restricted|unrestricted> - unrestricted - any MIB variable that
      has read/write access can be set; restricted (default) - MIB
      variables cannot be set, only read.
```

Supported Values:

- **Operator** -- The community can access all except the CONFIG MIB.
- **Manager** -- The community can access all MIB objects.

write-access

- [no] snmp-server community *COMMUNITY* < *Restricted* | *Unrestricted* | | ... >

```
Usage: [no] snmp-server community ASCII-STR
                    [manager|operator] [restricted|unrestricted]

Description: Add/delete SNMP community.

Parameters:

    o community ASCII-STR - Enter up to 32 characters to name an SNMP
      community.

    o <manager|operator> - manager - the community can access all MIB
      objects; operator (default) - the community can access all except
      the CONFIG MIB.

    o <restricted|unrestricted> - unrestricted - any MIB variable that
      has read/write access can be set; restricted (default) - MIB
      variables cannot be set, only read.
```

Supported Values:

- **Restricted** -- MIB variables cannot be set, only read.
- **Unrestricted** -- Any MIB variable that has read/write access can be set.
-
- **Unrestricted**

© 2007 Hewlett-Packard Development Company, L.P.

snmpv3

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] snmpv3 <community|group|notify|params|restricted-access|
                    targetaddress|user>

Description: Configure SNMPv3 features.
```

COMMAND STRUCTURE

- [no] snmpv3 **community** -- Configure SNMPv3 Community entry. **(p. 406)**
  - **index** -- Set community index. (ASCII-STR) **(p. 407)**
    - **name** -- Set community name. (ASCII-STR) **(p. 408)**
      - **sec-name** -- Set security name. (ASCII-STR) **(p. 410)**
        - **tag** -- Set tag value for the community (ASCII-STR) **(p. 411)**
- [no] snmpv3 **enable** -- Enable SNMPv3. **(p. 406)**
- [no] snmpv3 **group < ManagerPriv | ManagerAuth | OperatorAuth | ... >** -- Configure SNMPv3 User to Group entry. **(p. 406)**
  - **user** -- Set user to be added to the group. (ASCII-STR) **(p. 411)**
    - **sec-model < ver1 | ver2c | ver3 >** -- Set security model to be used. **(p. 410)**
- [no] snmpv3 **notify** -- Configure SNMPv3 Notification entry. (ASCII-STR) **(p. 408)**
  - **tagvalue** -- Set tag value that selects entries in the snmpTargetAddr table. (ASCII-STR) **(p. 411)**
- [no] snmpv3 **only** -- Accept only SNMP v3 messages. **(p. 408)**
- [no] snmpv3 **params** -- Configure SNMPv3 Target Parameter entry. (ASCII-STR) **(p. 408)**
  - **user** -- Set user that the switch will send messages on behalf. (ASCII-STR) **(p. 411)**
    - **sec-model** -- Set security model. **(p. 410)**
      - **sec-model12c < ver1 | ver2c >** -- Configure SNMPv3 User entry. **(p. 410)**
        - **message-processing < ver1 | ver2c | ver3 >** -- Set message processing model value. **(p. 407)**
      - **ver3** -- SNMP version 3 security model. **(p. 412)**
        - **message-processing** -- Set message processing model value. **(p. 407)**
          - **ver3 < noauth | auth | priv >** -- Set security level. **(p. 412)**
- [no] snmpv3 **restricted-access** -- Configure SNMPv1 and SNMPv2c access properties. **(p. 410)**
- [no] snmpv3 **targetaddress** -- Configure SNMPv3 Target Address entry. (ASCII-STR) **(p. 411)**
  - **params** -- Set parameter name. (ASCII-STR) **(p. 408)**
    - **ipaddr** -- Set IP address of the destination target. (IP-ADDR) **(p. 407)**
      - **addr-mask** -- Set range of transport addresses with this mask. (IP-ADDR) **(p. 405)**
      - **filter < None | Debug | All | ... >** -- Set log filters. **(p. 406)**
      - **max-msg-size < 484 to 65535 >** -- Set maximum message size value; default is 1472. **(p. 407)**
      - **port-mask** -- Set range of udp ports with this mask. (TCP/UDP-PORT) **(p. 408)**
      - **retries < 0 to 255 >** -- Set retries value; default is 3. **(p. 410)**
      - **taglist** -- Set list of values used to select this entry from snmpNotifyTable. (ASCII-STR) **(p. 411)**
      - **timeout < 0 to 2147483647 >** -- Set time-out value; default is 1500. **(p. 411)**
      - **udp-port** -- Set UDP port number to which the messages are sent; default is 162. (TCP/UDP-PORT) **(p. 411)**

© 2007 Hewlett-Packard Development Company, L.P.

- [no] snmpv3 **user** -- Configure SNMPv3 User entry. (ASCII-STR) **(p. 411)**
  - **auth** -- Set authentication paramaters. **(p. 405)**
    - **authpassword** -- Set authentication password. (ASCII-STR) **(p. 405)**
      - **priv** -- Set Privacy password. **(p. 409)**
        - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 409)**
        - **privprotocol < DES | AES >** -- Set privacy protocol. **(p. 409)**
          - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 409)**
    - **authprotocol < MD5 | SHA >** -- Set authentication protocol. **(p. 406)**
      - **authpassword** -- Set authentication password. (ASCII-STR) **(p. 405)**
        - **priv** -- Set Privacy password. **(p. 409)**
          - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 409)**
          - **privprotocol < DES | AES >** -- Set privacy protocol. **(p. 409)**
            - **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 409)**

COMMAND DETAILS

addr-mask (p. 405)	**message-processing (p. 407)**	**sec-model (p. 410)**
auth (p. 405)	**name (p. 408)**	**sec-model12c (p. 410)**
authpassword (p. 405)	**notify (p. 408)**	**sec-name (p. 410)**
authprotocol (p. 406)	**only (p. 408)**	**tag (p. 411)**
community (p. 406)	**params (p. 408)**	**taglist (p. 411)**
enable (p. 406)	**port-mask (p. 408)**	**tagvalue (p. 411)**
filter (p. 406)	**priv (p. 409)**	**targetaddress (p. 411)**
group (p. 406)	**privpassword (p. 409)**	**timeout (p. 411)**
index (p. 407)	**privprotocol (p. 409)**	**udp-port (p. 411)**
ipaddr (p. 407)	**restricted-access (p. 410)**	**user (p. 411)**
max-msg-size (p. 407)	**retries (p. 410)**	**ver3 (p. 412)**

addr-mask

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* addr-mask *IP-ADDR*

```
Set range of transport addresses with this mask.
```

auth

- snmpv3 user *USER* auth

```
Set authentication paramaters.
```

Next Available Options:
- **authpassword** -- Set authentication password. (ASCII-STR) **(p. 405)**
- **authprotocol** < MD5 | SHA > -- Set authentication protocol. **(p. 406)**

authpassword

- snmpv3 user *USER* auth *AUTHPASSWORD*

```
Set authentication password.
```

Next Available Option:
- **priv** -- Set Privacy password. **(p. 409)**

- snmpv3 user *USER* auth *< MD5 | SHA > AUTHPASSWORD*

© 2007 Hewlett-Packard Development Company, L.P.

```
Set authentication password.
```

Next Available Option:
- **priv** -- Set Privacy password. **(p. 409)**

authprotocol

- snmpv3 user *USER* auth *< MD5 | SHA >*

```
Set authentication protocol.
```

Supported Values:
- **MD5** -- Set the authentication protocol to md5.
- **SHA** -- Set the authentication protocol to sha.

Next Available Option:
- **authpassword** -- Set authentication password. (ASCII-STR) **(p. 405)**

community

- [no] snmpv3 community

```
Configure SNMPv3 Community entry.
```

Next Available Option:
- **index** -- Set community index. (ASCII-STR) **(p. 407)**

enable

- [no] snmpv3 enable

```
Enable SNMPv3.
```

filter

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* filter *< None | Debug | All | ... >*

```
Set log filters.
```

Supported Values:
- **None** -- Send no log messages.
- **Debug** -- Send debug traps (for Internal use).
- **All** -- Send all log messages
- **Not-INFO** -- Send all but informational-only messages.
- **Critical** -- Send critical-level log messages.

group

- [no] snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >*

```
Configure SNMPv3 User to Group entry.
```

Supported Values:
- **ManagerPriv** -- Require privacy and authentication, can access all objects.
- **ManagerAuth** -- Require authentication, can access all objects.

© 2007 Hewlett-Packard Development Company, L.P.

- **OperatorAuth** -- Requires authentication, limited access to objects.
- **OperatorNoAuth** -- No authentication required, limited access to objects.
- **ComManagerRW** -- Community with manager and unrestricted write access.
- **ComManagerR** -- Community with manager and restricted write access.
- **ComOperatorRW** -- Community with operator and unrestricted write access.
- **ComOperatorR** -- Community with operator and restricted write access.

Next Available Option:
- **user** -- Set user to be added to the group. (ASCII-STR) **(p. 411)**

index

- [no] snmpv3 community index *INDEX*

```
Set community index.
```

Next Available Option:
- **name** -- Set community name. (ASCII-STR) **(p. 408)**

ipaddr

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR*

```
Set IP address of the destination target.
```

Next Available Options:
- **addr-mask** -- Set range of transport addresses with this mask. (IP-ADDR) **(p. 405)**
- **filter** < None | Debug | All | ... > -- Set log filters. **(p. 406)**
- **max-msg-size** < 484 to 65535 > -- Set maximum message size value; default is 1472. **(p. 407)**
- **port-mask** -- Set range of udp ports with this mask. (TCP/UDP-PORT) **(p. 408)**
- **retries** < 0 to 255 > -- Set retries value; default is 3. **(p. 410)**
- **timeout** < 0 to 2147483647 > -- Set time-out value; default is 1500. **(p. 411)**
- **taglist** -- Set list of values used to select this entry from snmpNotifyTable. (ASCII-STR) **(p. 411)**
- **udp-port** -- Set UDP port number to which the messages are sent; default is 162. (TCP/UDP-PORT) **(p. 411)**

max-msg-size

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* max-msg-size *< 484 to 65535 >*

```
Set maximum message size value; default is 1472.
```

Range: < 484 to 65535 >

message-processing

- snmpv3 params *PARAMS* user *USER* sec-model *< ver1 | ver2c >* message-processing *< ver1 | ver2c | ver3 >*

```
Set message processing model value.
```

Supported Values:
- **ver1** -- SNMP version 1 message processing model.
- **ver2c** -- SNMP version 2c message processing model.

© 2007 Hewlett-Packard Development Company, L.P.

- **ver3** -- SNMP version 3 message processing model.

■ snmpv3 params *PARAMS* user *USER* sec-model ver3 message-processing

```
Set message processing model value.
```

Next Available Option:
- **ver3** < noauth | auth | priv > -- Set security level. **(p. 412)**

name

■ snmpv3 community index *INDEX* name *NAME*

```
Set community name.
```

Next Available Option:
- **sec-name** -- Set security name. (ASCII-STR) **(p. 410)**

notify

■ [no] snmpv3 notify *NOTIFY*

```
Configure SNMPv3 Notification entry.
```

Next Available Option:
- **tagvalue** -- Set tag value that selects entries in the snmpTargetAddr table. (ASCII-STR) **(p. 411)**

only

■ [no] snmpv3 only

```
Accept only SNMP v3 messages.
```

params

■ [no] snmpv3 params *PARAMS*

```
Configure SNMPv3 Target Parameter entry.
```

Next Available Option:
- **user** -- Set user that the switch will send messages on behalf. (ASCII-STR) **(p. 411)**

■ snmpv3 targetaddress *TARGETADDRESS* params *PARAMS*

```
Set parameter name.
```

Next Available Option:
- **ipaddr** -- Set IP address of the destination target. (IP-ADDR) **(p. 407)**

port-mask

■ snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* port-mask *TCP/UDP-PORT*

```
Set range of udp ports with this mask.
```

© 2007 Hewlett-Packard Development Company, L.P.

priv

- snmpv3 user *USER* auth *AUTHPASSWORD* priv

```
Set Privacy password.
```

Next Available Options:
- **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 409)**
- **privprotocol** < DES | AES > -- Set privacy protocol. **(p. 409)**

- snmpv3 user *USER* auth *< MD5 | SHA > AUTHPASSWORD* priv

```
Set Privacy password.
```

Next Available Options:
- **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 409)**
- **privprotocol** < DES | AES > -- Set privacy protocol. **(p. 409)**

privpassword

- snmpv3 user *USER* auth *AUTHPASSWORD* priv *PRIVPASSWORD*

```
Set Privacy password.
```

- snmpv3 user *USER* auth *AUTHPASSWORD* priv *< DES | AES > PRIVPASSWORD*

```
Set Privacy password.
```

- snmpv3 user *USER* auth *< MD5 | SHA > AUTHPASSWORD* priv *PRIVPASSWORD*

```
Set Privacy password.
```

- snmpv3 user *USER* auth *< MD5 | SHA > AUTHPASSWORD* priv *< DES | AES > PRIVPASSWORD*

```
Set Privacy password.
```

privprotocol

- snmpv3 user *USER* auth *AUTHPASSWORD* priv *< DES | AES >*

```
Set privacy protocol.
```

Supported Values:
- **DES** -- Set the privacy protocol to des.
- **AES** -- Set the privacy protocol to aes-128.

Next Available Option:
- **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 409)**

- snmpv3 user *USER* auth *< MD5 | SHA > AUTHPASSWORD* priv *< DES | AES >*

```
Set privacy protocol.
```

Supported Values:
- **DES** -- Set the privacy protocol to des.
- **AES** -- Set the privacy protocol to aes-128.

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **privpassword** -- Set Privacy password. (ASCII-STR) **(p. 409)**

restricted-access

- [no] snmpv3 restricted-access

```
Configure SNMPv1 and SNMPv2c access properties.
```

retries

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* retries *< 0 to 255 >*

```
Set retries value; default is 3.
```

Range: < 0 to 255 >

sec-model

- [no] snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* user *USER* sec-model *< ver1 | ver2c | ver3 >*

```
Set security model to be used.
```

Supported Values:
- **ver1** -- SNMP version 1 security model.
- **ver2c** -- SNMP version v2c security model.
- **ver3** -- SNMP version 3 security model.

- snmpv3 params *PARAMS* user *USER* sec-model

```
Set security model.
```

Next Available Options:
- **sec-model12c** < ver1 | ver2c > -- Configure SNMPv3 User entry.**(p. 410)**
- **ver3** -- SNMP version 3 security model.**(p. 412)**

sec-model12c

- snmpv3 params *PARAMS* user *USER* sec-model *< ver1 | ver2c >*

```
Configure SNMPv3 User entry.
```

Supported Values:
- **ver1** -- SNMP version 1 security model.
- **ver2c** -- SNMP version 2c security model.

Next Available Option:
- **message-processing** < ver1 | ver2c | ver3 > -- Set message processing model value. **(p. 407)**

sec-name

- snmpv3 community index *INDEX* name *NAME* sec-name *SEC-NAME*

```
Set security name.
```

Next Available Option:

© 2007 Hewlett-Packard Development Company, L.P.

- **tag** -- Set tag value for the community (ASCII-STR) **(p. 411)**

tag

- snmpv3 community index *INDEX* name *NAME* sec-name *SEC-NAME* tag *TAG*

  Set tag value for the community

taglist

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* taglist *TAGLIST*

  Set list of values used to select this entry from snmpNotifyTable.

tagvalue

- snmpv3 notify *NOTIFY* tagvalue *TAGVALUE*

  Set tag value that selects entries in the snmpTargetAddr table.

targetaddress

- [no] snmpv3 targetaddress *TARGETADDRESS*

  Configure SNMPv3 Target Address entry.

  Next Available Option:
  - **params** -- Set parameter name. (ASCII-STR) **(p. 408)**

timeout

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* timeout *< 0 to 2147483647 >*

  Set time-out value; default is 1500.

  Range: < 0 to 2147483647 >

udp-port

- snmpv3 targetaddress *TARGETADDRESS* params *PARAMS IP-ADDR* udp-port *TCP/UDP-PORT*

  Set UDP port number to which the messages are sent; default is 162.

user

- [no] snmpv3 group *< ManagerPriv | ManagerAuth | OperatorAuth | ... >* user *USER*

  Set user to be added to the group.

  Next Available Option:
  - **sec-model** < ver1 | ver2c | ver3 > -- Set security model to be used. **(p. 410)**

- snmpv3 params *PARAMS* user *USER*

  Set user that the switch will send messages on behalf.

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **sec-model** -- Set security model. **(p. 410)**

■ [no] snmpv3 user *USER*

```
Configure SNMPv3 User entry.
```

Next Available Option:
- **auth** -- Set authentication paramaters. **(p. 405)**

ver3

■ snmpv3 params *PARAMS* user *USER* sec-model ver3

```
SNMP version 3 security model.
```

Next Available Option:
- **message-processing** -- Set message processing model value. **(p. 407)**

■ snmpv3 params *PARAMS* user *USER* sec-model ver3 message-processing ver3 *< noauth | auth | priv >*

```
Set security level.
```

Supported Values:
- **noauth** -- no authentication (and no privacy)
- **auth** -- authentication (no privacy)
- **priv** -- authentication and privacy

© 2007 Hewlett-Packard Development Company, L.P.

sntp

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	timesync (page 447)

```
Usage: [no] sntp [broadcast|unicast]
       [no] sntp server IP-ADDR [version]
       sntp poll-interval <30-720>

Description: Configure the Simple Network Time Protocol (SNTP).

             The first version of the command specifies whether the
             switch operates in broadcast or unicast mode. If no mode is
             specified then the mode defaults to broadcast.

             The second version of the command adds or deletes an SNTP
             server to or from the configuration. The maximum number of
             SNTP servers that can be configured is 3. Version can have
             a value between 1 and 7. If no version is specified then a
             default value of 3 is used.

             The final version of this command sets the SNTP poll
             interval, which specifies the amount of time between updates
             of the system clock via SNTP.
```

COMMAND STRUCTURE

- sntp **broadcast** -- Operate in broadcast mode (p. 413)
- sntp **poll-interval < 30 to 720 >** -- The amount of time between updates of the system clock via SNTP (p. 414)
- [no] sntp **server** -- Configure SNTP servers to poll time from. (IP-ADDR) (p. 414)
  - **version < 1 to 7 >** -- Version of the SNTP server. (p. 414)
- sntp **unicast** -- Operate in unicast mode (p. 414)

EXAMPLES

Example: sntp poll-interval SECONDS

Change the SNTP poll interval to 300 seconds:

```
HPswitch(config)# sntp poll-interval 300
```

COMMAND DETAILS

broadcast (p. 413)	server (p. 414)	version (p. 414)
poll-interval (p. 414)	unicast (p. 414)	

broadcast

- sntp broadcast

```
Operate in broadcast mode
```

© 2007 Hewlett-Packard Development Company, L.P.

poll-interval

- sntp *< 30 to 720 >*

  `The amount of time between updates of the system clock via SNTP`

  Range: < 30 to 720 >

server

- [no] sntp server *IP-ADDR*

  `Configure SNTP servers to poll time from.`

  Next Available Option:
  - **version** < 1 to 7 > -- Version of the SNTP server.**(p. 414)**

unicast

- sntp unicast

  `Operate in unicast mode`

version

- sntp server *IP-ADDR < 1 to 7 >*

  `Version of the SNTP server.`

  Range: < 1 to 7 >

© 2007 Hewlett-Packard Development Company, L.P.

spanning-tree

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] spanning-tree [[ethernet] PORT-LIST ...]
             [pending ...]
             [instance ...]
             [legacy-mode]
             [legacy-path-cost]
             [config-name ASCII-STR]
             [config-revision <0-65535>]
             [max-hops <1-40>]
             [force-version <stp-compatible|rstp-operation|mstp-operation>]
             [trap <errant-bpdu>]
             [forward-delay <4-30>]
             [hello-time <1-10>]
             [maximum-age <6-40>]
             [bpdu-filter]
             [bpdu-protection]
             [priority <<0-15>|<0-65535>>]

Description: Set the parameters for operation of the switch in a spanning tree
             topology.
             Note - the default spanning tree configuration complies with the
             IEEE 802.1s, Multiple Spanning Tree Protocol (MSTP), standard
             recommended values and should not be changed without thorough
             knowledge of spanning tree operation.
             If 'no' is used the command disables the spanning tree operation.
             Parameters are not allowed with 'no' option.

Parameters:

    o ethernet PORT-LIST ... - Configure the port-specific parameters.
      Use 'spanning-tree [ethernet] PORT-LIST ?' to get a list of all
      possible configuration options, or 'spanning-tree [ethernet]
      PORT-LIST help' to get a detailed help for this form of the command.
    o force-version (default: native mode) - Set Spanning Tree protocol
      compatibility mode on the device. Forces current protocol engine to
      emulate behavior of earlier versions of spanning tree protocol or
      operate in the native mode. The value of this parameter applies to
      all ports of the switch.
    o forward-delay <4-30> (default: 15) - Time (in seconds) the switch
      waits between transitioning from listening to learning and from
      learning to forwarding states.
    o hello-time <1-10> (default: 2) - Time (in seconds) between messages
      transmitted when the switch is root. The parameter is in force
      for all switch ports in RSTP and STP modes. If the MSTP engine is
      running this global value can be changed for individual ports.
    o maximum-age <6-40> (default: 20) - Maximum message age (in seconds)
      of received STP information before it is discarded.
    o priority <0-15> or <0-65535> (default is 32768 and step 8 respectively) -
      The device priority - used along with the switch MAC address to determine
```

© 2007 Hewlett-Packard Development Company, L.P.

```
   which device is the root. If 802.1w or 802.1s STP version is set, then
   the range of 0-61440 is divided into steps of 4096. These steps are
   numbered from 0 to 15.
 o config-name ASCII-STR (default is switch's MAC address) - The name of
   the MST region configuration identifier. The name has the maximum length
   of 32 characters and is case sensitive. Use "no" form of the command
   to reset to the default name. The parameter is configurable in MSTP mode
   only.
 o config-revision <0-65535> (default is 0) - The revision number of the MST
   region configuration identifier. The parameter is configurable in MSTP
   mode only.
 o max-hops <1-40> (default is 20) - The number of hops in the MST region
   before the MST BPDU is discarded and the information held for a port is
   aged. This parameter is configurable in MSTP mode only and serves for
   the same purpose as the maximum-age and message-age couple used by
   legacy single spanning tree bridges.
 o instance ... - Allows to create, delete and configure MST instances.
   This command is available in MSTP mode only. See the command help for
   further details.
 o pending ... - Manipulate the pending MSTP configuration. This command
   is available in MSTP mode only. See the command help for more details.
 o legacy-path-cost - Set default pathcosts to 802.1d (legacy)  or 802.1t
   (not legacy) values. This command is available in MSTP mode only.
 o legacy-mode - Set spanning-tree protocol to operate either in 802.1d
   legacy mode or in 802.1s native mode. This command is available in MSTP
   mode only. See the command help for more details.
 o trap - Enable/disable STP traps. The following traps are generated
          as a result of finding an unusual condition on a switch port.
          Possible trap names are:
        - 'errant-bpdu' signifies that an unexpected Spanning Tree BPDU
          has been received on a port.
```

COMMAND STRUCTURE

- spanning-tree **bpdu-protection-timeout < 0 to 65535 >** -- Set time between messages transmission when the switch is root. **(p. 419)**
- [no] spanning-tree **config-name** -- Set the MST region configuration name (default is switch's MAC address). **(p. 419)**
  - **config-name** -- Specify the configuration name (maximum 32 characters). (ASCII-STR) **(p. 419)**
- spanning-tree **config-revision < 0 to 65535 >** -- Set the MST region configuration revision number (default is 0). **(p. 420)**
- spanning-tree **force-version < STP-compatible | RSTP-operation >** -- Set Spanning Tree protocol compatibility mode. **(p. 420)**
- spanning-tree **force-version < STP-compatible | RSTP-operation | MSTP-operation >** -- Set Spanning Tree protocol compatibility mode. **(p. 420)**
- spanning-tree **forward-delay < 4 to 30 >** -- Set time the switch waits between transitioning from listening to learning and from learning to forwarding states. **(p. 420)**
- spanning-tree **hello-time < 1 to 10 >** -- Set time between messages transmission when the switch is root. **(p. 420)**
- [no] spanning-tree **instance** -- Create, delete or configure an MST instance **(p. 421)**
  - **INSTANCE_ID < 1 to 16 >** -- ID of the MST instance to configure. **(p. 421)**
    - **port-list** -- Configure MST instance ports parameters ([ethernet] PORT-LIST) **(p. 425)**
      - **path-cost** -- Set the port pathcost for the instance (default is 'auto'). **(p. 423)**
        - **auto** -- Use dynamic method of selecting a value for the path cost. **(p. 418)**
        - **path-cost < 1 to 200000000 >** -- Set port's path cost to the fixed value. **(p. 423)**
      - **priority < 0 to 15 >** -- Set the port priority for the instance (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8). **(p. 429)**

© 2007 Hewlett-Packard Development Company, L.P.

- **priority < 0 to 15 >** -- Set the device priority for the MST instance (the value is in range of 0-61440 divided into steps of 4096 that are numbered from 0 to 15, default is step 8). **(p. 429)**
- **vlan** -- Configure VLANs for the MST instance. **(p. 429)**
  - **VLAN-ID-RANGE** -- VLAN(s) to add to or to remove from the MST instance (VLAN-ID-RANGE) **(p. 430)**

- **ist** -- Configure internal spanning tree (IST) instance. **(p. 422)**
  - **port-list** -- Configure internal spanning tree (IST) instance ports parameters ([ethernet] PORT-LIST) **(p. 425)**
    - **path-cost** -- Set the internal port pathcost for the IST (default is 'auto'). **(p. 423)**
      - **auto** -- Use dynamic method of selecting a value for the path cost. **(p. 418)**
      - **path-cost < 1 to 200000000 >** -- Set port's path cost to the fixed value. **(p. 423)**

- [no] spanning-tree **legacy-mode** -- Set spanning-tree protocol to operate either in 802.1d legacy mode or in 802.1s native mode. 'spanning-tree legacy-mode' is the equivalent of executing: spanning-tree legacy-path-cost spanning-tree force-version stp-compatible 'no spanning-tree legacy-mode' is the equivalent of executing: no spanning-tree legacy-path-cost spanning-tree force-version mstp-operation **(p. 422)**
- [no] spanning-tree **legacy-path-cost** -- Set 802.1d (legacy) or 802.1t (not legacy) default pathcost values. **(p. 422)**
- spanning-tree **max-hops < 1 to 40 >** -- Set the max number of hops in a region before the MST BPDU is discarded and the information held for a port is aged (default is 20). **(p. 422)**
- spanning-tree **maximum-age < 6 to 40 >** -- Set maximum age of received STP information before it is discarded. **(p. 423)**
- [no] spanning-tree **pending** -- Manipulate pending MSTP configuration **(p. 424)**
  - **apply** -- Apply pending MSTP configuration (swaps active and pending configuratons). **(p. 418)**
  - **config-name** -- Set the pending MST region configuration name (default is switch's MAC address). **(p. 419)**
    - **config-name** -- Specify the configuration name (maximum 32 characters). (ASCII-STR) **(p. 419)**
  - **config-revision < 0 to 65535 >** -- Set the pending MST region configuration revision number (default is 0). **(p. 420)**
  - **instance** -- Change pending MST instance configuration. **(p. 421)**
    - **INSTANCE_ID < 1 to 16 >** -- ID of the MST instance to configure. **(p. 421)**
      - **vlan** -- Configure VLANs for the MST instance. **(p. 429)**
        - **VLAN-ID-RANGE** -- VLAN(s) to add to or to remove from the MST instance (VLAN-ID-RANGE) **(p. 430)**
  - **reset** -- Copy active configuration to pending. **(p. 429)**
- [no] spanning-tree **port-list** -- Configure the port-specific parameters of the spanning tree protocol for individual ports ([ethernet] PORT-LIST) **(p. 425)**
  - **bpdu-filter** -- Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a continuous fowarding state. **(p. 419)**
  - **bpdu-protection** -- Disable the specific port or ports if the port(s) receives STP BPDUs. **(p. 419)**
  - **edge-port** -- Set that port is connected to a LAN segment that does not have any bridge connected to it. **(p. 420)**
  - **hello-time** -- Set message transmission interval (in sec.) on the port. **(p. 420)**
    - **global** -- Use the globally configured hello-time value. **(p. 420)**
    - **hello-time < 1 to 10 >** -- Set message transmission interval (in sec.) on the port. **(p. 420)**
  - **mcheck** -- Force the port to transmit RST BPDUs. **(p. 423)**
  - **path-cost** -- Set port's path cost value. **(p. 423)**
    - **auto** -- Use dynamic method of selecting a value for the path cost. **(p. 418)**
    - **path-cost < 1 to 200000000 >** -- Set port's path cost to the fixed value. **(p. 423)**
    - **path-cost < 1 to 65535 >** -- Set port's path cost to the fixed value. **(p. 423)**
  - **point-to-point-mac < Force-True | Force-False | Auto >** -- Set if the port is connected to a point-to-point segment or not. **(p. 425)**

© 2007 Hewlett-Packard Development Company, L.P.

  - **priority < 0 to 15 >** -- Set port priority (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8). **(p. 429)**
- [no] spanning-tree **port-list** -- Configure the port-specific parameters of the spanning tree protocol for individual ports ([ethernet] PORT-LIST) **(p. 425)**
  - **bpdu-filter** -- Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a continuous fowarding state. **(p. 419)**
  - **bpdu-protection** -- Disable the specific port or ports if the port(s) receives STP BPDUs. **(p. 419)**
  - **mode < Norm | Fast | Uplink >** -- Set spanning tree operation mode. **(p. 423)**
  - **path-cost** -- Set port's path cost value. **(p. 423)**
    - **auto** -- Use dynamic method of selecting a value for the path cost. **(p. 418)**
    - **path-cost < 1 to 200000000 >** -- Set port's path cost to the fixed value. **(p. 423)**
    - **path-cost < 1 to 65535 >** -- Set port's path cost to the fixed value. **(p. 423)**
  - **priority < 0 to 255 >** -- Set port priority (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8). **(p. 429)**
- spanning-tree **priority < 0 to 65535 >** -- Set the device STP priority. **(p. 429)**
- spanning-tree **priority < 0 to 15 >** -- Set the device STP priority (the value is in range of 0-61440 divided into steps of 4096 that are numbered from 0 to 15, default is step 8). **(p. 429)**
- [no] spanning-tree **trap < errant-bpdu >** -- Enable/disable STP traps. **(p. 429)**

COMMAND DETAILS

apply (p. 418)	**global (p. 420)**	**mode (p. 423)**
auto (p. 418)	**hello-time (p. 420)**	**path-cost (p. 423)**
bpdu-filter (p. 419)	**instance (p. 421)**	**pending (p. 424)**
bpdu-protection (p. 419)	**INSTANCE_ID (p. 421)**	**point-to-point-mac (p. 425)**
bpdu-protection-timeout (p. 419)	**ist (p. 422)**	**port-list (p. 425)**
config-name (p. 419)	**legacy-mode (p. 422)**	**priority (p. 429)**
config-revision (p. 420)	**legacy-path-cost (p. 422)**	**reset (p. 429)**
edge-port (p. 420)	**max-hops (p. 422)**	**trap (p. 429)**
force-version (p. 420)	**maximum-age (p. 423)**	**vlan (p. 429)**
forward-delay (p. 420)	**mcheck (p. 423)**	**VLAN-ID-RANGE (p. 430)**

apply

- spanning-tree pending apply

```
Apply pending MSTP configuration (swaps active and pending configuratons).
```

auto

- spanning-tree *[ETHERNET] PORT-LIST* path-cost auto

```
Use dynamic method of selecting a value for the path cost.
```

- spanning-tree *[ETHERNET] PORT-LIST* path-cost auto

```
Use dynamic method of selecting a value for the path cost.
```

- spanning-tree instance ist *[ETHERNET] PORT-LIST* path-cost auto

```
Use dynamic method of selecting a value for the path cost.
```

- spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST* path-cost auto

```
Use dynamic method of selecting a value for the path cost.
```

© 2007 Hewlett-Packard Development Company, L.P.

bpdu-filter

- [no] spanning-tree *[ETHERNET] PORT-LIST* bpdu-filter

```
Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a
 continuous fowarding state.
```

- [no] spanning-tree *[ETHERNET] PORT-LIST* bpdu-filter

```
Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a
 continuous fowarding state.
```

bpdu-protection

- [no] spanning-tree *[ETHERNET] PORT-LIST* bpdu-protection

```
Disable the specific port or ports if the port(s) receives STP BPDUs.
```

- [no] spanning-tree *[ETHERNET] PORT-LIST* bpdu-protection

```
Disable the specific port or ports if the port(s) receives STP BPDUs.
```

Caution

Ports configured with the BPDU filter mode remain active (learning and forwarding frames); however, spanning-tree cannot receive or transmit BPDUs on the port. The port remains in a forwarding state, permitting all broadcast traffic. This can create a network storm if there are any loops (that is, trunks or redundant links) using these ports. If you suddenly have a high load, disconnect the link and disable the bpdu-filter (using the "no" command).

bpdu-protection-timeout

- spanning-tree bpdu-protection-timeout *< 0 to 65535 >*

```
Set time between messages transmission when the switch is root.
```

Range: < 0 to 65535 >

config-name

- [no] spanning-tree config-name

```
Set the MST region configuration name (default is switch's MAC address).
```

Next Available Option:

- **config-name** -- Specify the configuration name (maximum 32 characters). (ASCII-STR) **(p. 419)**

- spanning-tree config-name *CONFIG-NAME*

```
Specify the configuration name (maximum 32 characters).
```

- [no] spanning-tree pending config-name

```
Set the pending MST region configuration name (default is switch's MAC address).
```

Next Available Option:

- **config-name** -- Specify the configuration name (maximum 32 characters). (ASCII-STR) **(p. 419)**

- spanning-tree pending config-name *CONFIG-NAME*

© 2007 Hewlett-Packard Development Company, L.P.

```
Specify the configuration name (maximum 32 characters).
```

config-revision

- spanning-tree config-revision *< 0 to 65535 >*

```
Set the MST region configuration revision number (default is 0).
```

Range: < 0 to 65535 >

- spanning-tree pending config-revision *< 0 to 65535 >*

```
Set the pending MST region configuration revision number (default is 0).
```

Range: < 0 to 65535 >

edge-port

- [no] spanning-tree *[ETHERNET] PORT-LIST* edge-port

```
Set that port is connected to a LAN segment that does not have any bridge connected
to it.
```

force-version

- spanning-tree force-version *< STP-compatible | RSTP-operation >*

```
Set Spanning Tree protocol compatibility mode.
```

Supported Values:
- **STP-compatible** -- The protocol operates as STP on all ports.
- **RSTP-operation** -- The protocol operates as Rapid STP on all ports except those ports where a system that is using 802.1d Spanning Tree has been detected.

- spanning-tree force-version *< STP-compatible | RSTP-operation | MSTP-operation >*

```
Set Spanning Tree protocol compatibility mode.
```

Supported Values:
- **STP-compatible** -- The protocol operates as STP on all ports.
- **RSTP-operation** -- The protocol operates as Rapid STP on all ports except those ports where a system that is using 802.1d Spanning Tree has been detected.
- **MSTP-operation** -- The protocol operates as Multiple STP on all ports where compatibility to the old STP protocol versions is not required.

forward-delay

- spanning-tree forward-delay *< 4 to 30 >*

```
Set time the switch waits between transitioning from listening to learning and from
learning to forwarding states.
```

Range: < 4 to 30 >

global

- spanning-tree *[ETHERNET] PORT-LIST* hello-time global

```
Use the globally configured hello-time value.
```

hello-time

- spanning-tree *[ETHERNET] PORT-LIST* hello-time

© 2007 Hewlett-Packard Development Company, L.P.

```
Set message transmission interval (in sec.) on the port.
```

Next Available Options:
- **hello-time** < 1 to 10 > -- Set message transmission interval (in sec.) on the port.**(p. 420)**
- **global** -- Use the globally configured hello-time value.**(p. 420)**

- spanning-tree *[ETHERNET] PORT-LIST* hello-time *< 1 to 10 >*

```
Set message transmission interval (in sec.) on the port.
```

Range: < 1 to 10 >

- spanning-tree hello-time *< 1 to 10 >*

```
Set time between messages transmission when the switch is root.
```

Range: < 1 to 10 >

instance

- spanning-tree instance

```
Usage: spanning-tree instance <ist|<1-16>> vlan VLAN-ID [VLAN-ID ...]
       [no] spanning-tree instance <1-16>
       [no] spanning-tree instance <ist|1-16> ...

Description: Create, delete or configure an MST instance.
             The first form of the command is used to create a new
             instance or map VLAN(s) to an existent one. Each instance
             must have at least one VLAN mapped to it. The VLANs
             unmapped from other instances are automatically mapped to
             the IST instance. Only IST VLANs can be directly mapped to
             other instances. When VLANs are mapped to an instance they
             are automatically unmapped from the instance they were
             mapped to before. The second form of the command deletes
             an instance. The IST instance cannot be deleted. The third
             form of the command can be used to configure an existent
             instance. Follow the third form of the command with '?' to
             get a complete list of all the configurable parameters and
             sub-commands.
```

Next Available Options:
- **ist** -- Configure internal spanning tree (IST) instance.**(p. 422)**
- **INSTANCE_ID** < 1 to 16 > -- ID of the MST instance to configure.**(p. 421)**

- spanning-tree pending instance

```
Change pending MST instance configuration.
```

Next Available Option:
- **INSTANCE_ID** < 1 to 16 > -- ID of the MST instance to configure.**(p. 421)**

INSTANCE_ID

- [no] spanning-tree instance *< 1 to 16 >*

```
ID of the MST instance to configure.
```

© 2007 Hewlett-Packard Development Company, L.P.

Range: < 1 to 16 >

Next Available Options:
- **vlan** -- Configure VLANs for the MST instance.**(p. 429)**
- **priority** < 0 to 15 > -- Set the device priority for the MST instance (the value is in range of 0-61440 divided into steps of 4096 that are numbered from 0 to 15, default is step 8).**(p. 429)**
- **port-list** -- Configure MST instance ports parameters ([ethernet] PORT-LIST) **(p. 425)**

■ [no] spanning-tree pending instance *< 1 to 16 >*

```
ID of the MST instance to configure.
```

Range: < 1 to 16 >

Next Available Option:
- **vlan** -- Configure VLANs for the MST instance.**(p. 429)**

ist

■ spanning-tree instance ist

```
Configure internal spanning tree (IST) instance.
```

Next Available Option:
- **port-list** -- Configure internal spanning tree (IST) instance ports parameters ([ethernet] PORT-LIST) **(p. 425)**

legacy-mode

■ [no] spanning-tree legacy-mode

```
Set spanning-tree protocol to operate either in 802.1d legacy
mode or in 802.1s native mode.
'spanning-tree legacy-mode' is the equivalent of executing:
     spanning-tree legacy-path-cost
     spanning-tree force-version stp-compatible
'no spanning-tree legacy-mode' is the equivalent of executing:
     no spanning-tree legacy-path-cost
     spanning-tree force-version mstp-operation
```

legacy-path-cost

■ [no] spanning-tree legacy-path-cost

```
Set 802.1d (legacy) or 802.1t (not legacy) default pathcost values.
```

max-hops

■ spanning-tree max-hops *< 1 to 40 >*

```
Set the max number of hops in a region before the MST BPDU is discarded and the
information held for a port is aged (default is 20).
```

Range: < 1 to 40 >

© 2007 Hewlett-Packard Development Company, L.P.

maximum-age

- spanning-tree maximum-age *< 6 to 40 >*

  `Set maximum age of received STP information before it is discarded.`

  Range: < 6 to 40 >

mcheck

- [no] spanning-tree *[ETHERNET] PORT-LIST* mcheck

  `Force the port to transmit RST BPDUs.`

mode

- spanning-tree *[ETHERNET] PORT-LIST* mode *< Norm | Fast | Uplink >*

  `Set spanning tree operation mode.`

  Supported Values:
  - **Norm** -- Normal spanning tree mode.
  - **Fast** -- Fast spanning tree mode.
  - **Uplink** -- Fast Uplink spanning tree mode.

path-cost

- spanning-tree *[ETHERNET] PORT-LIST* path-cost

  `Set port's path cost value.`

  Next Available Options:
  - **path-cost** < 1 to 200000000 > -- Set port's path cost to the fixed value.**(p. 423)**
  - **path-cost** < 1 to 65535 > -- Set port's path cost to the fixed value.**(p. 423)**
  - **auto** -- Use dynamic method of selecting a value for the path cost.**(p. 418)**

- spanning-tree *[ETHERNET] PORT-LIST* path-cost *< 1 to 200000000 >*

  `Set port's path cost to the fixed value.`

  Range: < 1 to 200000000 >
- spanning-tree *[ETHERNET] PORT-LIST* path-cost *< 1 to 65535 >*

  `Set port's path cost to the fixed value.`

  Range: < 1 to 65535 >
- spanning-tree *[ETHERNET] PORT-LIST* path-cost

  `Set port's path cost value.`

  Next Available Options:
  - **path-cost** < 1 to 200000000 > -- Set port's path cost to the fixed value.**(p. 423)**
  - **path-cost** < 1 to 65535 > -- Set port's path cost to the fixed value.**(p. 423)**
  - **auto** -- Use dynamic method of selecting a value for the path cost.**(p. 418)**

- spanning-tree *[ETHERNET] PORT-LIST* path-cost *< 1 to 200000000 >*

  `Set port's path cost to the fixed value.`

© 2007 Hewlett-Packard Development Company, L.P.

Range: < 1 to 200000000 >

- spanning-tree *[ETHERNET] PORT-LIST* path-cost *< 1 to 65535 >*

```
Set port's path cost to the fixed value.
```

Range: < 1 to 65535 >

- spanning-tree instance ist *[ETHERNET] PORT-LIST* path-cost

```
Set the internal port pathcost for the IST (default is 'auto').
```

Next Available Options:

- **path-cost** < 1 to 200000000 > -- Set port's path cost to the fixed value.**(p. 423)**
- **auto** -- Use dynamic method of selecting a value for the path cost.**(p. 418)**

- spanning-tree instance ist *[ETHERNET] PORT-LIST* path-cost *< 1 to 200000000 >*

```
Set port's path cost to the fixed value.
```

Range: < 1 to 200000000 >

- spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST* path-cost

```
Set the port pathcost for the instance (default is 'auto').
```

Next Available Options:

- **path-cost** < 1 to 200000000 > -- Set port's path cost to the fixed value.**(p. 423)**
- **auto** -- Use dynamic method of selecting a value for the path cost.**(p. 418)**

- spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST* path-cost *< 1 to 200000000 >*

```
Set port's path cost to the fixed value.
```

Range: < 1 to 200000000 >

pending

- spanning-tree pending

```
Usage: spanning-tree pending <apply|reset>
       [no] spanning-tree pending [...]

Description: Manipulate pending MSTP configuration. The pending
             configuration can be modified without affecting current
             spanning tree operation. The 'spanning-tree pending apply'
             command runs the pending configuration consistency check
             and activates the pending configuration if it yields no
             consistency errors. The pending and active configurations
             exchange places if the 'apply' command is completed
             successfully.
             The 'spanning-tree pending reset' command overrides pending
             configuration with the active one.
             Not all spanning tree parameters are available for the pending
             configuration. The parameters that are not available for the
             pending configuration are not affected or when must be
             implicitly set are initialized to the defaults. Use
             'spanning-tree pending ?' to get a complete list of all
             supported pending configuration commands and parameters.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **apply** -- Apply pending MSTP configuration (swaps active and pending configuratons).**(p. 418)**
- **reset** -- Copy active configuration to pending.**(p. 429)**
- **config-name** -- Set the pending MST region configuration name (default is switch's MAC address).**(p. 419)**
- **config-revision** < 0 to 65535 > -- Set the pending MST region configuration revision number (default is 0).**(p. 420)**
- **instance** -- Change pending MST instance configuration.**(p. 421)**

point-to-point-mac

- spanning-tree *[ETHERNET] PORT-LIST* point-to-point-mac *< Force-True | Force-False | Auto >*

```
Set if the port is connected to a point-to-point segment or not.
```

Supported Values:

- **Force-True** -- Treat the port as if it is connected to a point-to-point LAN segment.
- **Force-False** -- Treat the port as if it is connected to a non-point-to-point LAN segment.
- **Auto** -- Determine automatically status of the segment connected to the port.

port-list

- [no] spanning-tree *[ETHERNET] PORT-LIST*

```
Usage: spanning-tree [ethernet] PORT-LIST <<edge-port>|<mcheck>|
                            <mode <norm|fast|uplink>>|
                            <path-cost <1-65535>|<1-200000000>|auto>>|
                            <point-to-point <force-true|force-false|auto>>|
                            <bpdu-filter>|
                            <bpdu-protection>|
                            <hello-time <1-10>>|
                            <priority <0-15>>>

Description: Configure the port-specific parameters of the spanning
             tree protocol for individual ports.

Parameters:
    o edge-port - Applies only to RSTP/MSTP. When correctly set for each
      port it improves the protocol operation. Indicate whether the port is
      connected to LAN segment that doesn't have any bridge or switch
      connected to it. If a bridge or switch is detected on the segment,
      the port will automatically operate as if Edge = 'No' has been set.
    o mcheck - Applies only to RSTP/MSTP. Forces the port to transmit RST
      or MST BPDUs. This option improves the operation of RSTP/MSTP.
      For any port that is connected to a bridge or switch that is known
      to be using STP (not RSTP or MSTP), MCheck should be set to 'No'.
    o mode <norm|fast|uplink> (default: norm) - Applies only to STP.
      'Norm' (for normal) mode causes the port to operate according to the
      standard Spanning Tree Protocol - when connected, the port progresses
      through the Listening, Learning, and either Blocking or Forwarding
      states. 'Fast' mode causes the port to immediately operate in the
      Forwarding State when a device is connected to it. Use this setting
      only on ports that are connected to end nodes (for example: PCs,
      Workstation, or printers). Caution: Changing the Mode to 'Fast' on ports
      connected to a hub or switch may cause loops in your network that STP
      may not be able to detect in all cases.
      'Uplink' Note: The spanning-tree uplink mode is intended for use by
      network administrators who have a strong understanding of STP operation.
      Also, uplink mode should only be used in the edge switches in a network
```

© 2007 Hewlett-Packard Development Company, L.P.

```
   environment.
o  path-cost <1-65535> or <1-200000000> or <auto> - Individual port cost -
   used to determine which ports are forwarding ports.
   Can be set to 'auto' or configured by a user. A value of 'auto' (default)
   indicates the link speed determines the cost value. The following ranges
   are available for user configuration:
   For RSTP/MSTP: 1 through 200000000 (recommended value is 2000000 for
   Ethernet and 10/100TX ports operating at 10 Mbps; 200000 for 10/100TX
   ports operating at 100 Mbps and 100FX; 20000 for 1000SX, 1000LX,
   1000Stk, 1000T ports).
   For STP: 1 through 65535 (recommended value is 100 for Ethernet and
   10/100TX ports operating at 10 Mbps; 10 for 10/100TX ports operating
   at 100 Mbps and 100FX; 5 for 1000SX, 1000LX, 1000Stk, 1000T ports).
o  bpdu-filter (default: off) - On/off control to ignore a port's
   incoming spanning-tree BPDU packets and prevent sending any.
o  bpdu-protection (default: disabled) - Enable/Disable STP BPDU
   protection on port(s). If bpdu-protection is enabled on specified
   port(s) and if the port(s) receives spanning-tree BPDU packets then
   the port(s) will be disabled.
o  point-to-point <force-true|force-false|auto> (default: auto) - Applies
   only to RSTP. When correctly set for each port, it improves the operation
   of RSTP. 'Force-True' indicates that the port will be treated as if it is
   connected to a point-to-point LAN segment, regardless of any information
   to the contrary that the switch receives. 'Force-False' indicates that
   the port will be treated as if it is connected to a non-point-to-point
   LAN segment, regardless of any information to the contrary that the
   switch receives. Set 'Force-False' on any port that is known to be
   connected to a hub, bridge, or another switch. 'Auto' value indicates
   that the administrator requires the point-to-point status of the MAC
   to be determined in accordance with the specific MAC procedures.
o  priority <0-15> (default: 8 ) -  Another value used by spanning tree
   to select the forwarding ports. The port with the lowest number has
   the highest priority. The range of 0-240 is divided into 16 steps. These
   steps are numbered from 0 to 15. The number entered is multiplied to 16
   to calculate the priority value to use by the protocol if protocol
   version is other than standard STP (802.1d).
o  priority <0-15> (default: 8 ) - Another value used by spanning tree
   protocol to select the forwarding ports. The range of 0-240 is divided
   into 16 steps that are numbered from 0 to 15. These steps are used as
   the value to enter. The lowest value means the highest priority for the
   port.
o  hello-time <<1-10>|global> (default: global) - Time (in seconds)
   between message transmissions when the switch is root. Available for
   the per-port configuration in MSTP mode only. The value 'global' means
   to use globally configured hello-time for the port.
```

Next Available Options:

- **edge-port** -- Set that port is connected to a LAN segment that does not have any bridge connected to it.**(p. 420)**
- **mcheck** -- Force the port to transmit RST BPDUs.**(p. 423)**
- **path-cost** -- Set port's path cost value.**(p. 423)**
- **point-to-point-mac** < Force-True | Force-False | Auto > -- Set if the port is connected to a point-to-point segment or not.**(p. 425)**
- **priority** < 0 to 15 > -- Set port priority (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8).**(p. 429)**
- **hello-time** -- Set message transmission interval (in sec.) on the port.**(p. 420)**
- **bpdu-filter** -- Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a continuous fowarding state.**(p. 419)**

© 2007 Hewlett-Packard Development Company, L.P.

- **bpdu-protection** -- Disable the specific port or ports if the port(s) receives STP BPDUs.**(p. 419)**

■ spanning-tree *[ETHERNET] PORT-LIST*

```
Usage: spanning-tree [ethernet] PORT-LIST <<edge-port>|<mcheck>|
                            <mode <norm|fast|uplink>>|
                            <path-cost <1-65535>|<1-200000000>|auto>>|
                            <point-to-point <force-true|force-false|auto>>|
                            <bpdu-filter>|
                            <bpdu-protection>|
                            <hello-time <1-10>>|
                            <priority <0-15>>>

Description: Configure the port-specific parameters of the spanning
             tree protocol for individual ports.

Parameters:
    o edge-port - Applies only to RSTP/MSTP. When correctly set for each
      port it improves the protocol operation. Indicate whether the port is
      connected to LAN segment that doesn't have any bridge or switch
      connected to it. If a bridge or switch is detected on the segment,
      the port will automatically operate as if Edge = 'No' has been set.
    o mcheck - Applies only to RSTP/MSTP. Forces the port to transmit RST
      or MST BPDUs. This option improves the operation of RSTP/MSTP.
      For any port that is connected to a bridge or switch that is known
      to be using STP (not RSTP or MSTP), MCheck should be set to 'No'.
    o mode <norm|fast|uplink> (default: norm) - Applies only to STP.
      'Norm' (for normal) mode causes the port to operate according to the
      standard Spanning Tree Protocol - when connected, the port progresses
      through the Listening, Learning, and either Blocking or Forwarding
      states. 'Fast' mode causes the port to immediately operate in the
      Forwarding State when a device is connected to it. Use this setting
      only on ports that are connected to end nodes (for example: PCs,
      Workstation, or printers). Caution: Changing the Mode to 'Fast' on ports
      connected to a hub or switch may cause loops in your network that STP
      may not be able to detect in all cases.
      'Uplink' Note: The spanning-tree uplink mode is intended for use by
      network administrators who have a strong understanding of STP operation.
      Also, uplink mode should only be used in the edge switches in a network
      environment.
    o path-cost <1-65535> or <1-200000000> or <auto> - Individual port cost -
      used to determine which ports are forwarding ports.
      Can be set to 'auto' or configured by a user. A value of 'auto' (default)
      indicates the link speed determines the cost value. The following ranges
      are available for user configuration:
      For RSTP/MSTP: 1 through 200000000 (recommended value is 2000000 for
      Ethernet and 10/100TX ports operating at 10 Mbps; 200000 for 10/100TX
      ports operating at 100 Mbps and 100FX; 20000 for 1000SX, 1000LX,
      1000Stk, 1000T ports).
      For STP: 1 through 65535 (recommended value is 100 for Ethernet and
      10/100TX ports operating at 10 Mbps; 10 for 10/100TX ports operating
      at 100 Mbps and 100FX; 5 for 1000SX, 1000LX, 1000Stk, 1000T ports).
    o bpdu-filter (default: off) - On/off control to ignore a port's
      incoming spanning-tree BPDU packets and prevent sending any.
    o bpdu-protection (default: disabled) - Enable/Disable STP BPDU
      protection on port(s). If bpdu-protection is enabled on specified
      port(s) and if the port(s) receives spanning-tree BPDU packets then
      the port(s) will be disabled.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
  o point-to-point <force-true|force-false|auto> (default: auto) - Applies
    only to RSTP. When correctly set for each port, it improves the operation
    of RSTP. 'Force-True' indicates that the port will be treated as if it is
    connected to a point-to-point LAN segment, regardless of any information
    to the contrary that the switch receives. 'Force-False' indicates that
    the port will be treated as if it is connected to a non-point-to-point
    LAN segment, regardless of any information to the contrary that the
    switch receives. Set 'Force-False' on any port that is known to be
    connected to a hub, bridge, or another switch. 'Auto' value indicates
    that the administrator requires the point-to-point status of the MAC
    to be determined in accordance with the specific MAC procedures.
  o priority <0-15> (default: 8 ) -  Another value used by spanning tree
    to select the forwarding ports. The port with the lowest number has
    the highest priority. The range of 0-240 is divided into 16 steps. These
    steps are numbered from 0 to 15. The number entered is multiplied to 16
    to calculate the priority value to use by the protocol if protocol
    version is other than standard STP (802.1d).
  o priority <0-15> (default: 8 ) - Another value used by spanning tree
    protocol to select the forwarding ports. The range of 0-240 is divided
    into 16 steps that are numbered from 0 to 15. These steps are used as
    the value to enter. The lowest value means the highest priority for the
    port.
  o hello-time <<1-10>|global> (default: global) - Time (in seconds)
    between message transmissions when the switch is root. Available for
    the per-port configuration in MSTP mode only. The value 'global' means
    to use globally configured hello-time for the port.
```

Next Available Options:

- **mode** < Norm | Fast | Uplink > -- Set spanning tree operation mode.**(p. 423)**
- **path-cost** -- Set port's path cost value.**(p. 423)**
- **priority** < 0 to 255 > -- Set port priority (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8).**(p. 429)**
- **bpdu-protection** -- Disable the specific port or ports if the port(s) receives STP BPDUs.**(p. 419)**
- **bpdu-filter** -- Stop a specific port or ports from transmitting BPDUs, receiving BPDUs, and assume a continuous fowarding state.**(p. 419)**

■ spanning-tree instance ist *[ETHERNET] PORT-LIST*

```
Usage: spanning-tree ist [ethernet] PORT-LIST ...

Description: Configure internal spanning tree (IST) instance ports parameters.
             Follow the PORT-LIST with the '?' to get the list of all
             possible options.
```

Next Available Option:

- **path-cost** -- Set the internal port pathcost for the IST (default is 'auto').**(p. 423)**

■ spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST*

```
Usage: spanning-tree instance <1-16> [ethernet] PORT-LIST ...

Description: Configure MST instance ports parameters. Follow the PORT-LIST
             with the '?' to get the list of all possible options.
```

Next Available Options:

- **path-cost** -- Set the port pathcost for the instance (default is 'auto').**(p. 423)**

© 2007 Hewlett-Packard Development Company, L.P.

- **priority** < 0 to 15 > -- Set the port priority for the instance (the value is in range of 0-240 divided into steps of 16 that are numbered from 0 to 15, default is step 8).**(p. 429)**

priority

- spanning-tree *[ETHERNET] PORT-LIST* priority *< 0 to 15 >*

  ```
  Set port priority (the value is in range of 0-240 divided into steps of 16 that are
  numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 15 >
- spanning-tree *[ETHERNET] PORT-LIST* priority *< 0 to 255 >*

  ```
  Set port priority (the value is in range of 0-240 divided into steps of 16 that are
  numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 255 >
- spanning-tree priority *< 0 to 65535 >*

  ```
  Set the device STP priority.
  ```

  Range: < 0 to 65535 >
- spanning-tree priority *< 0 to 15 >*

  ```
  Set the device STP priority (the value is in range of 0-61440 divided into steps of
  4096 that are numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 15 >
- spanning-tree instance *< 1 to 16 >* priority *< 0 to 15 >*

  ```
  Set the device priority for the MST instance (the value is in range of 0-61440 divided
   into steps of 4096 that are numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 15 >
- spanning-tree instance *< 1 to 16 > [ETHERNET] PORT-LIST* priority *< 0 to 15 >*

  ```
  Set the port priority for the instance (the value is in range of 0-240 divided into
  steps of 16 that are numbered from 0 to 15, default is step 8).
  ```

  Range: < 0 to 15 >

reset

- spanning-tree pending reset

  ```
  Copy active configuration to pending.
  ```

trap

- [no] spanning-tree trap *< errant-bpdu >*

  ```
  Enable/disable STP traps.
  ```

  Supported Values:
  - **errant-bpdu**

vlan

- spanning-tree instance *< 1 to 16 >* vlan

© 2007 Hewlett-Packard Development Company, L.P.

```
Configure VLANs for the MST instance.
```

Next Available Option:

- **VLAN-ID-RANGE** -- VLAN(s) to add to or to remove from the MST instance (VLAN-ID-RANGE) **(p. 430)**

- spanning-tree pending instance *< 1 to 16 >* vlan

```
Configure VLANs for the MST instance.
```

Next Available Option:

- **VLAN-ID-RANGE** -- VLAN(s) to add to or to remove from the MST instance (VLAN-ID-RANGE) **(p. 430)**

VLAN-ID-RANGE

- [no] spanning-tree instance *< 1 to 16 >* vlan *VLAN-ID-RANGE*

```
VLAN(s) to add to or to remove from the MST instance
```

- [no] spanning-tree pending instance *< 1 to 16 >* vlan *VLAN-ID-RANGE*

```
VLAN(s) to add to or to remove from the MST instance
```

© 2007 Hewlett-Packard Development Company, L.P.

stack

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage:  [no] stack
        [no] stack commander ASCII-STR
        [no] stack join MAC-ADDR
        [no] stack member INTEGER mac-address MAC-ADDR [password ASCII-STR]
        [no] stack auto-join
        [no] stack auto-grab
             stack transmission-interval <1-300>

Description: Configure device to/from a stack - a group of devices manageable
             as a single entity.
          -  'stack' by itself enables stacking on the switch. The 'no' option
             disables stacking.
          -  'stack commander' configures the switch to be a 'commander switch'
             given the name specified in the ASCII-STR parameter. The 'no'
             option disables the commander function. The 'commander switch' can
             be used as a single point of access for configuring and monitoring
             all the switches in the stack.
          -  'stack join' causes the switch, as a candidate switch, to join the
             stack whose commander switch is identified by the MAC-ADDR
             parameter. The 'no' option causes the switch to leave that stack.
          -  'stack member' causes a candidate switch identified by the
             MAC-ADDR to be an INTEGER-th member of this switch's stack in case
             of this switch is a commander. The INTEGER number must be between
             1 and 15 (0 is reserved for the commander switch). Password must
             be supplied if the candidate switch has a manager password.
          -  'stack auto-join' allows this switch, being a candidate, to
             automatically join a stack. The 'no' option disables this feature.
          -  'stack auto-grab' allows this switch, being a commander, to
             automatically incorporate candidates. The 'no' option disables
             this feature.
          -  'stack transmission-interval' sets the transmission-interval (in
             seconds) between the sending out of new discovery packets. The
             default value is 60 seconds.
```

COMMAND STRUCTURE

- [no] stack **auto-grab** -- Configure commander to incorporate candidates **(p. 432)**
- [no] stack **auto-join** -- Allow this switch to automatically join a stack **(p. 432)**
- [no] stack **commander** -- Configure this switch to be a commander (ASCII-STR) **(p. 432)**
- [no] stack **join** -- Join a stack as a member (MAC-ADDR) **(p. 432)**
- [no] stack **member** -- Incorporate candidate into stack **(p. 432)**
  - **mac-address** -- MAC address of candidate (MAC-ADDR) **(p. 432)**
  - **password** -- Manager password of candidate (ASCII-STR) **(p. 432)**
- stack **transmission-interval** **< 1 to 300 >** -- Transmission interval of HP discovery packets **(p. 432)**

© 2007 Hewlett-Packard Development Company, L.P.

COMMAND DETAILS

auto-grab (p. 432)	join (p. 432)	password (p. 432)
auto-join (p. 432)	mac-address (p. 432)	transmission-interval (p. 432)
commander (p. 432)	member (p. 432)	

auto-grab

- [no] stack auto-grab

```
Configure commander to incorporate candidates
```

auto-join

- [no] stack auto-join

```
Allow this switch to automatically join a stack
```

commander

- [no] stack commander *COMMANDER*

```
Configure this switch to be a commander
```

join

- [no] stack join *MAC-ADDR*

```
Join a stack as a member
```

mac-address

- stack member *INTEGER* mac-address *MAC-ADDR*

```
MAC address of candidate
```

member

- [no] stack member *INTEGER*

```
Incorporate candidate into stack
```

Next Available Options:

- **mac-address** -- MAC address of candidate (MAC-ADDR) **(p. 432)**
- **password** -- Manager password of candidate (ASCII-STR) **(p. 432)**

password

- stack member *INTEGER* password *PASSWORD*

```
Manager password of candidate
```

transmission-interval

- stack transmission-interval *< 1 to 300 >*

```
Transmission interval of HP discovery packets
```

Range: < 1 to 300 >

© 2007 Hewlett-Packard Development Company, L.P.

startup-default

OVERVIEW

Category:	manager
Primary context:	manager
Related Commands	show flash (page 350)

```
Usage: startup-default [<primary|secondary>] config FILENAME

Description: Set the default configuration file.  A separate configuration
             file may be set as the default for each software image, or a
             single configuration file may be set as the default when
             booting either image by omitting the optional 'primary|secondary'
             parameter.
```

COMMAND STRUCTURE

- startup-default **config < config1 >** -- Specify configuration file to set as default. **(p. 433)**
- startup-default **image < primary | secondary >** -- **(p. 433)**
  - **config < config1 >** -- Specify configuration file to set as default. **(p. 433)**

COMMAND DETAILS

config (p. 433)	**image (p. 433)**

config

- startup-default *< primary | secondary >* config *< config1>*

  ```
  Specify configuration file to set as default.
  ```

  Supported Values:
  - **config1**
- startup-default config *< config1>*

  ```
  Specify configuration file to set as default.
  ```

  Supported Values:
  - **config1**

image

- startup-default *< primary | secondary >*

  Supported Values:
  - **primary** -- Primary flash image.
  - **secondary** -- Secondary flash image.

  Next Available Option:
  - **config** < config1 > -- Specify configuration file to set as default.**(p. 433)**

© 2007 Hewlett-Packard Development Company, L.P.

static-mac

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**show static-mac (page 382)**

```
Usage: static-mac <MAC-ADDR> vlan <VLAN-ID> interface <PORT-LIST>

Description: Lock down a MAC address to a port on a vlan. The switch will forward traffic

             addressed to the MAC address only on the port and VLAN to which the address
 is
              locked.

Parameters:

    o MAC-ADDR  - MAC address to lock down.

    o vlan VLAN-ID - VLAN on which to lock down the MAC address.

    o interface PORT-LIST - Port list on which to lock down the MAC address.

Examples:

    (1) ProCurve#  static-mac 0800095F3AD6 vlan V1 interface A1
```

COMMAND STRUCTURE

- [no] static-mac MAC-ADDR **interface** -- The port list on which to lock down the MAC address. ([ethernet] PORT-NUM) **(p. 434)**
- [no] static-mac MAC-ADDR **vlan** -- The VLAN ID on which to lock down the MAC address. (VLAN-ID) **(p. 435)**

EXAMPLES

Example: static-mac MAC-ADDR <...>

Lock MAC address 0800095F3AD6 to port A1 on VLAN V1:

```
ProCurve# static-mac 0800095F3AD6 vlan V1 interface A1
```

COMMAND DETAILS

interface (p. 434)	**vlan (p. 435)**

interface

- [no] static-mac *MAC-ADDR* interface *[ETHERNET] PORT-NUM*

  The port list on which to lock down the MAC address.

© 2007 Hewlett-Packard Development Company, L.P.

vlan

- [no] static-mac *MAC-ADDR* vlan *VLAN-ID*

  The VLAN ID on which to lock down the MAC address.

© 2007 Hewlett-Packard Development Company, L.P.

static-vlan

OVERVIEW

Category:	config
Primary context:	config
Related Commands	**show vlan (page 390)** **show gvrp (page 351)** **gvrp (page 150)**

```
Usage: static-vlan VLAN-ID

Description: Transform a dynamic VLAN to a static VLAN.
```

EXAMPLES

Example: static-vlan

Convert dynamically created VLAN 125 into a port-based, static VLAN:

```
ProCurve(config)# static-vlan 125
```

tacacs-server

OVERVIEW

Category:	Accounting
Primary context:	config
Related Commands	**show tacacs (page 384)**

```
Usage:  [no] tacacs-server host IP-ADDR [key KEY-STR]
        [no] tacacs-server key KEY-STR
             tacacs-server timeout <1-255>

Description: Configure TACACS+ authentication servers.
             The first version of the command adds (or removes, if 'no' is
             specified) a TACACS+ server to (from) the list of servers that
             will be used for authentication. Up to 3 TACACS+ servers can be
             configured. If 'key' is specified then this command also sets
             (or removes) an encryption key used during the authentication
             session with given server.
             The second version sets (or removes, with 'no') the global
             encryption key for TACACS+ authentication.
             The last version sets the response timeout interval for
             TACACS+ server.

Parameters:

    o address IP-ADDR [key KEY-STR] - Specifies the IP address of the
              server to use. Optional parameter 'key KEY-STR' specifies
              an encryption key used during the authentication session with
              given server. Specifying this key overrides the key set by
              the global configuration 'tacacs-server key KEY-STR' command
              for this server only.
    o key KEY-STR - Up to 100 characters. Encryption key used for TACACS+
              authentication. Default value is null, which means TACACS+
              packets are sent using clear text. The KEY-STR parameter is
              not allowed when a key is removed.
    o timeout <1-255> - Sets the timeout interval in seconds the TACACS+
              server must send response back to the switch.
              If this interval expires and no response the next configured
              server is queried. Default value is 5 seconds.
```

COMMAND STRUCTURE

- [no] tacacs-server **host** -- IP address of the server to use. (IP-ADDR) **(p. 438)**
  - **key** -- Encryption key to use with server. **(p. 438)**
    - **key** -- (ASCII-STR) **(p. 438)**
- [no] tacacs-server **key** -- Global encryption key. **(p. 438)**
  - **key** -- (ASCII-STR) **(p. 438)**
- tacacs-server **timeout < 1 to 255 >** -- Server timeout interval. **(p. 439)**

© 2007 Hewlett-Packard Development Company, L.P.

EXAMPLES

Example: tacacs-server host

Delete a per-server encryption key in the switch, and re-enter the 'tacacs-server host' command without the key parameter. For example, if you have north01 configured as the encryption key for a TACACS+ server with an IP address of 10.28.227.104 and you want to eliminate the key, use this command:

```
ProCurve(config)# tacacs-server host 10.28.227.104
```

Example: tacacs-server host key

Configure north01 as a per-server encryption key:

```
ProCurve(config)# tacacs-server host 10.28.227.63 key north01
```

Example: tacacs-server key

Configure north01 as a global encryption key:

```
ProCurve(config) tacacs-server key north01
```

Example: tacacs-server timeout

Change the timeout period from 5 seconds (the default) to 3 seconds:

```
HPswitch(config)# tacacs-server timeout 3
```

COMMAND DETAILS

host (p. 438) **key (p. 438)** **timeout (p. 439)**

host

- [no] tacacs-server host *IP-ADDR*

```
IP address of the server to use.
```

Next Available Option:
- **key** -- Encryption key to use with server.**(p. 438)**

key

- [no] tacacs-server host *IP-ADDR* key

```
Encryption key to use with server.
```

Next Available Option:
- **key** -- (ASCII-STR) **(p. 438)**

- tacacs-server host *IP-ADDR* key *KEY*
- [no] tacacs-server key

```
Global encryption key.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:

- **key** -- (ASCII-STR) **(p. 438)**

- tacacs-server key *KEY*

timeout

- tacacs-server timeout *< 1 to 255 >*

  `Server timeout interval.`

  Range: < 1 to 255 >

© 2007 Hewlett-Packard Development Company, L.P.

telnet

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	

```
Usage: telnet <IP-ADDR|SWITCH-NUM>

Description: Initiate an outbound telnet session to another network device.
             The destination can be specified either by IP address of the
             device, or, if the switch is a commander switch in a stack, by
             the identifier of another member switch in the stack.
```

COMMAND STRUCTURE

- telnet **ip-addr** -- IP address of the telnet server to connect. (IP-ADDR) **(p. 440)**
- telnet **SWITCH-NUM** -- The stack member number to which to telnet. (NUMBER) **(p. 440)**

EXAMPLES

Example: telnet IP-ADDR

Establish a Telnet session with the device at IP address 10.0.0.2:

```
ProCurve(config)# telnet 10.0.0.2
```

COMMAND DETAILS

ip-addr (p. 440)	**SWITCH-NUM (p. 440)**

ip-addr

- telnet *IP-ADDR*

```
IP address of the telnet server to connect.
```

SWITCH-NUM

- telnet *NUMBER*

```
The stack member number to which to telnet.
```

© 2007 Hewlett-Packard Development Company, L.P.

telnet-server

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show console (page 344)**

```
Usage: [no] telnet-server

Description: Enable/disable remote nodes to Telnet into the switch.
             To be accessed by Telnet, the switch must first be given an IP
             configuration. By default, the telnet access is enabled.
             Use 'show console' command to see the status of this function.
```

EXAMPLES

Example: telnet-server

Re-enable inbound Telnet access:

```
ProCurve(config)# telnet-server
```

© 2007 Hewlett-Packard Development Company, L.P.

terminal

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show terminal (page 386)**

```
Usage: terminal [length <2-1000> | width <53-1920>]

Description: Set the dimensions of the terminal window.
```

COMMAND STRUCTURE

- terminal **length < 2 to 1000 >** -- Set the height of the terminal window (NUMBER) **(p. 442)**
- terminal **width < 61 to 1920 >** -- Set the width of the terminal window (NUMBER) **(p. 442)**

COMMAND DETAILS

length (p. 442)	**width (p. 442)**

length

- terminal length *< 2 to 1000 >*

```
Usage: terminal length <2-1000>

Description: Set the height of the terminal window.
```

Range: < 2 to 1000 >

width

- terminal width *< 61 to 1920 >*

```
Usage: terminal width <53-1920>

Description: Set the width of the terminal window.
```

Range: < 61 to 1920 >

© 2007 Hewlett-Packard Development Company, L.P.

tftp

OVERVIEW

Category:	
Primary context:	config
Related Commands	

```
Usage: [no] tftp [client|server]

Description: Enable/disable TFTP, trivial file transfer protocol.
If stftp is enabled, tftp should be disabled. If
stftp is to be enabled via snmp, both tftp and
auto-tftp MUST first be disabled.
```

COMMAND STRUCTURE

- [no] tftp **client** -- Enable/Disable tftp client **(p. 443)**
- [no] tftp **server** -- Enable/Disable tftp server **(p. 443)**

COMMAND DETAILS

client (p. 443)	**server (p. 443)**

client

- [no] tftp client

```
Enable/Disable tftp client
```

server

- [no] tftp server

```
Enable/Disable tftp server
```

© 2007 Hewlett-Packard Development Company, L.P.

time

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**ip (page 180)** **sntp (page 413)** **clock (page 69)**

```
Usage: time [HH:MM:SS] [MM/DD[/[yy]yy]]
            [daylight-time-rule <none|alaska|continental-us-and-canada|
                                 middle-europe-and-portugal|
                                 southern-hemisphere|
                                 western-europe|user-defined>
                                 [begin-date <MM/DD>] [end-date <MM/DD>]
            [timezone <-720..840>]

Description: Display/set current time, date, and local time parameters.
             Called without any parameters displays the information
             mentioned above.

Parameters:
    o HH:MM:SS           - New time.
    o MM/DD[/[yy]yy]     - New date.
    o timezone           - The number of minutes your location is to the
                           West(-) or East(+) of GMT. Default is 0.
    o daylight-time-rule - The daylight savings time rule for your location.
                           'none' (default) disables daylight savings time.
                           'begin-date' and 'end-date' are valid only if the
                           daylight time rule is set to 'user-defined'.
    o begin-date         - Set the beginning date for daylight savings time.
    o end-date           - Set the ending dates for daylight savings time.
                           Daylight savings time adjustment will be made at
                           2:00 AM on the first Sunday on or after the
                           specified date.
```

COMMAND STRUCTURE

- time **begin-date** -- The begin date of daylight savings time (MM/DD) **(p. 445)**
- time **date** -- New date (MM/DD[/[YY]YY]) **(p. 445)**
- time **daylight-time-rule < None | Alaska | Continental-US-and-Canada | ... >** -- The daylight savings time rule for your location **(p. 445)**
- time **end-date** -- The end date of daylight savings time (MM/DD) **(p. 445)**
- time **time** -- New time (HH:MM[:SS]) **(p. 445)**
- time **timezone < -720 to 840 >** -- The number of minutes your location is West(-) or East(+) of GMT **(p. 445)**

EXAMPLES

Example: time MM/DD[/[YY]YY]

Set the time on the switch to 9:45 a.m. on November 17, 2002:

```
ProCurve(config)# time 9:45 11/17/02
```

© 2007 Hewlett-Packard Development Company, L.P.

Example: timesync sntp

Select SNTP as the time source 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):

```
ProCurve(config)# timesync sntp
```

Example: time timezone daylight-time-rule

Set the time zone and daylight time rule for Vancouver, Canada:

```
ProCurve(config)# time timezone -480 daylight-time-rule continental-us-and-canada
```

COMMAND DETAILS

begin-date (p. 445)	**daylight-time-rule (p. 445)**	**time (p. 445)**
date (p. 445)	**end-date (p. 445)**	**timezone (p. 445)**

begin-date

- time begin-date *MM/DD*

```
The begin date of daylight savings time
```

date

- time *[DATE]*

```
New date
```

daylight-time-rule

- time daylight-time-rule *< None | Alaska | Continental-US-and-Canada | ... >*

```
The daylight savings time rule for your location
```

Supported Values:

- **None**
- **Alaska**
- **Continental-US-and-Canada**
- **Middle-Europe-and-Portugal**
- **Southern-Hemisphere**
- **Western-Europe**
- **User-defined**

end-date

- time end-date *MM/DD*

```
The end date of daylight savings time
```

time

- time *[TIME]*

```
New time
```

timezone

- time timezone *< -720 to 840 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
The number of minutes your location is West(-) or East(+) of GMT
```

Range: < -720 to 840 >

© 2007 Hewlett-Packard Development Company, L.P.

timesync

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**ip (page 180)** **sntp (page 413)** **show timep (page 386)** **show sntp (page 381)**

```
Usage: [no] timesync <timep|sntp>

Description: Configure the network time protocol.
```

COMMAND STRUCTURE

- timesync **sntp** -- Set the time protocol to SNTP **(p. 447)**
- timesync **timep** -- Set the time protocol to the network time protocol **(p. 447)**

EXAMPLES

Example: timesync sntp

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):

```
ProCurve(config)# timesync sntp
ProCurve(config)# sntp unicast
ProCurve(config)# sntp server 10.28.227.141
```

COMMAND DETAILS

sntp (p. 447)	**timep (p. 447)**

sntp

- timesync sntp

```
Set the time protocol to SNTP
```

timep

- timesync timep

```
Set the time protocol to the network time protocol
```

© 2007 Hewlett-Packard Development Company, L.P.

traceroute

OVERVIEW

Category:	Switch Management
Primary context:	operator
Related Commands	ping (page 263)

```
Usage: traceroute <IP_ADDR | hostname> [minttl <1-255>]
                  [maxttl <1-255>] [timeout <1-120>]
                  [probes <1-5>]

Description: Trace the route to a device on the network.

Parameters:

   o IP-ADDR - Network IP address of station to which to send traceroute.

   o hostname - domain name of station to which to send traceroute.

   o [minttl <1-255>] - Minimum number of hops used in outgoing probe
     packets. The default value is 1.

   o [maxttl <1-255>] - Maximum number of hops used in outgoing probe
     packets. The default value is 30.

   o [timeout <1-120>] - Time (in seconds) to wait for a response to a
     probe. The default value is 5 seconds.

   o [probes <1-5>] - Number of probe queries to send out for each hop.
     The default value is 3.

Examples:

     (1)ProCurve# traceroute 1.1.1.1
```

COMMAND STRUCTURE

- traceroute **host-name** -- Domain name of the destination host. (ASCII-STR) (p. 449)
  - **maxttl < 1 to 255 >** -- Maximum time to live <1-255>. (p. 449)
  - **minttl < 1 to 255 >** -- Minimum time to live <1-255>. (p. 449)
  - **probes < 1 to 5 >** -- Number of Probes <1-5>. (p. 450)
  - **timeout < 1 to 120 >** -- Traceroute timeout in seconds <1-120>. (p. 450)
- traceroute **ip-addr** -- Destination IP address. (IP-ADDR) (p. 449)
  - **maxttl < 1 to 255 >** -- Maximum time to live <1-255>. (p. 449)
  - **minttl < 1 to 255 >** -- Minimum time to live <1-255>. (p. 449)
  - **probes < 1 to 5 >** -- Number of Probes <1-5>. (p. 450)
  - **timeout < 1 to 120 >** -- Traceroute timeout in seconds <1-120>. (p. 450)

EXAMPLES

Example: traceroute IP-ADDR

Trace the route to the device that has IP address 10.168.1.146:

© 2007 Hewlett-Packard Development Company, L.P.

```
ProCurve# traceroute 10.168.1.146
traceroute to 10.168.1.146 ,
             1 hop min, 30 hops max, 5 sec. timeout, 3 probes
 1 10.57.191.129          2 ms       3 ms       3 ms
 2 10.57.232.1            4 ms       2 ms       3 ms
 3 10.168.1.146           4 ms       3 ms       3 ms
```

COMMAND DETAILS

host-name (p. 449)	**maxttl (p. 449)**	**probes (p. 450)**
ip-addr (p. 449)	**minttl (p. 449)**	**timeout (p. 450)**

host-name

- traceroute *HOST-NAME*

```
Domain name of the destination host.
```

Next Available Options:

- **minttl** < 1 to 255 > -- Minimum time to live <1-255>.**(p. 449)**
- **maxttl** < 1 to 255 > -- Maximum time to live <1-255>.**(p. 449)**
- **timeout** < 1 to 120 > -- Traceroute timeout in seconds <1-120>.**(p. 450)**
- **probes** < 1 to 5 > -- Number of Probes <1-5>.**(p. 450)**

ip-addr

- traceroute *IP-ADDR*

```
Destination IP address.
```

Next Available Options:

- **minttl** < 1 to 255 > -- Minimum time to live <1-255>.**(p. 449)**
- **maxttl** < 1 to 255 > -- Maximum time to live <1-255>.**(p. 449)**
- **timeout** < 1 to 120 > -- Traceroute timeout in seconds <1-120>.**(p. 450)**
- **probes** < 1 to 5 > -- Number of Probes <1-5>.**(p. 450)**

maxttl

- traceroute *IP-ADDR* maxttl *< 1 to 255 >*

```
Maximum time to live <1-255>.
```

Range: < 1 to 255 >

- traceroute *HOST-NAME* maxttl *< 1 to 255 >*

```
Maximum time to live <1-255>.
```

Range: < 1 to 255 >

minttl

- traceroute *IP-ADDR* minttl *< 1 to 255 >*

```
Minimum time to live <1-255>.
```

Range: < 1 to 255 >

- traceroute *HOST-NAME* minttl *< 1 to 255 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Minimum time to live <1-255>.
```

Range: < 1 to 255 >

probes

- traceroute *IP-ADDR* probes *< 1 to 5 >*

```
Number of Probes <1-5>.
```

Range: < 1 to 5 >

- traceroute *HOST-NAME* probes *< 1 to 5 >*

```
Number of Probes <1-5>.
```

Range: < 1 to 5 >

timeout

- traceroute *IP-ADDR* timeout *< 1 to 120 >*

```
Traceroute timeout in seconds <1-120>.
```

Range: < 1 to 120 >

- traceroute *HOST-NAME* timeout *< 1 to 120 >*

```
Traceroute timeout in seconds <1-120>.
```

Range: < 1 to 120 >

© 2007 Hewlett-Packard Development Company, L.P.

trunk

OVERVIEW

Category:	Traffic Management
Primary context:	config
Related Commands	**show trunks (page 386)**

```
Usage: trunk [ethernet] PORT-LIST
             <trk1|trk2...trkN>
             [trunk|lacp]
       no trunk [ethernet] PORT-LIST

Description: Add or remove a switch port from a port trunk.
             Each port on the switch (up to 8 ports total) can be made
             a member of a port trunk. The 'no trunk' command can be used
             to remove ports from an existing trunk. The switch supports
             any one of the following trunk groups:

             Trunk - A static port grouping in which no protocols are used
             to create or maintain the trunk (type 'trunk').

             LACP - A port groping in which trunk membership is dynamically
             determined using the IEEE 802.1ad Link Aggregation Protocol.
             For LACP trunks the trunk group may instead be manually
             configured as static trunk.
             Manually configuring a static LACP trunk allows you to specify
             which ports are members and still configure advanced LACP
             features (type 'lacp').

             Any trunk group can have up to 8 member ports. All ports that
             belong to the same trunk group must have the same port type.
             All trunk groups use an algorithm that considers the source and
             destination MAC addresses for load distribution.

             General Considerations: To avoid broadcast storms, or
             loops in your network while configuring trunks, first
             disable or disconnect all the ports you wish to add or
             remove from both sides of the trunk.  Once done configuring
             the trunk, enable or re-connect the ports.
```

COMMAND STRUCTURE

- trunk **portlist** -- Specify the ports that are to be added to/removed from a trunk. ([ethernet] PORT-LIST) **(p. 452)**
  - **trunk-group < Trk1 | Trk2 | Trk3 | ... >** -- Specify the trunk group a port is to be a member of. **(p. 452)**
    - **type < Trunk | LACP | | ... >** -- Specify protocol to use on a manually configured trunk. **(p. 453)**

EXAMPLES

Example: trunk

Use ports C4 - C6 to create a non-protocol static trunk group with the group name of trk2:

© 2007 Hewlett-Packard Development Company, L.P.

```
ProCurve(config)# trunk c4-c6 trk2 trunk
```

COMMAND DETAILS

portlist (p. 452) trunk-group (p. 452) type (p. 453)

portlist

- trunk *[ETHERNET] PORT-LIST*

```
Specify the ports that are to be added to/removed from a trunk.
```

Next Available Option:

- **trunk-group** < Trk1 | Trk2 | Trk3 | ... > -- Specify the trunk group a port is to be a member of. **(p. 452)**

trunk-group

- trunk *[ETHERNET] PORT-LIST < Trk1 | Trk2 | Trk3 | ... >*

```
Specify the trunk group a port is to be a member of.
```

Supported Values:

- **Trk1** -- Trunk group 1
- **Trk2** -- Trunk group 2
- **Trk3** -- Trunk group 3
- **Trk4** -- Trunk group 4
- **Trk5** -- Trunk group 5
- **Trk6** -- Trunk group 6
- **Trk7** -- Trunk group 7
- **Trk8** -- Trunk group 8
- **Trk9** -- Trunk group 9
- **Trk10** -- Trunk group 10
- **Trk11** -- Trunk group 11
- **Trk12** -- Trunk group 12
- **Trk13** -- Trunk group 13
- **Trk14** -- Trunk group 14
- **Trk15** -- Trunk group 15
- **Trk16** -- Trunk group 16
- **Trk17** -- Trunk group 17
- **Trk18** -- Trunk group 18
- **Trk19** -- Trunk group 19
- **Trk20** -- Trunk group 20
- **Trk21** -- Trunk group 21
- **Trk22** -- Trunk group 22
- **Trk23** -- Trunk group 23
- **Trk24** -- Trunk group 24
- **Trk25** -- Trunk group 25
- **Trk26** -- Trunk group 26
- **Trk27** -- Trunk group 27
- **Trk28** -- Trunk group 28
- **Trk29** -- Trunk group 29
- **Trk30** -- Trunk group 30
- **Trk31** -- Trunk group 31
- **Trk32** -- Trunk group 32

© 2007 Hewlett-Packard Development Company, L.P.

- **Trk33** -- Trunk group 33
- **Trk34** -- Trunk group 34
- **Trk35** -- Trunk group 35
- **Trk36** -- Trunk group 36

Next Available Option:
- **type** < Trunk | LACP | | ... > -- Specify protocol to use on a manually configured trunk. **(p. 453)**

type

■ trunk *[ETHERNET] PORT-LIST < Trk1 | Trk2 | Trk3 | ... > < Trunk | LACP | | ... >*

```
Specify protocol to use on a manually configured trunk.
```

Supported Values:
- **Trunk** -- Do not use any protocol to create or maintain the trunk.
- **LACP** -- Use IEEE 802.1ad Link Aggregation protocol.
-
- **SA-Trunk**

© 2007 Hewlett-Packard Development Company, L.P.

update

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	

```
Usage: update

Description: Enter ROM update mode.
```

© 2007 Hewlett-Packard Development Company, L.P.

upgrade-software

OVERVIEW

Category:	
Primary context:	manager
Related Commands	

```
Usage: upgrade-software SOFTWARE-KEY

Description: Enter a key to upgrade system software and enable advanced
             features.
```

© 2007 Hewlett-Packard Development Company, L.P.

virus-throttle

OVERVIEW

Category:	Troubleshooting
Primary context:	config
Related Commands	**connection-rate-filter (page 73)**

```
Usage:       [no] virus-throttle

Description: To configure virus throttling, please use the 'connection-rate-filter'
command.
```

© 2007 Hewlett-Packard Development Company, L.P.

vlan

OVERVIEW

Category:	VLANs
Primary context:	config
Related Commands	**show vlans (page 391)** **ip (page 180)** **router (page 292)** **mirror-port (page 257)**

```
Usage: [no] vlan VLAN-ID [...]

Description: Add, delete, edit VLAN configuration or enter a VLAN context.
             If an existing VLAN-ID is specified you are put into the
             context for that VLAN, and can then execute commands for that
             VLAN. If a new VLAN-ID is specified, the new VLAN is added with
             the VLAN-ID, and you are put into the context of the new VLAN.
             If you follow the command with one of the VLAN Context commands
             in the same command line, the context level is not changed, but
             the commands are executed for the VLAN specified by the
             VLAN-ID. The 'no' option of the VLAN command is used to delete
             the VLAN specified by VLAN-ID.
```

COMMAND STRUCTURE

- vlan VLAN-ID **auto** -- Cause each port identified in the port list to learn its VLAN membership using the GARP VLAN Registration Protocol (GVRP) ([ethernet] PORT-LIST) **(p. 469)**
- vlan VLAN-ID **connection-rate-filter** -- Re-enables access to a host or set of hosts that has been previously blocked by the connection rate filter **(p. 470)**
  - **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 493)**
    - **all** -- Resets all previously blocked by the connection rate filter **(p. 465)**
    - **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 474)**
    - **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 491)**
- [no] vlan VLAN-ID **dhcp-snooping** -- **(p. 471)**
- [no] vlan VLAN-ID **forbid** -- Prevent ports from becoming a member of the current VLAN ([ethernet] PORT-LIST) **(p. 472)**
- [no] vlan VLAN-ID **igmp-proxy** -- Associate an IGMP proxy domain with a VLAN **(p. 475)**
  - **domain-name < END OF PRINTABLE >** -- Specify the domain name to associate/disassociate with the VLAN. (ASCII-STR) **(p. 471)**
- [no] vlan VLAN-ID **ip** -- Configure various IP parameters for the VLAN **(p. 476)**
  - **access-group** -- Apply the specified access control list on this VLAN interface (ASCII-STR) **(p. 463)**
    - **direction < in | out | connection-rate-filter | ... >** -- **(p. 471)**
  - **address** -- Set IP parameters for communication within an IP network **(p. 464)**
    - **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters. **(p. 471)**
    - **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 476)**
  - **forward-protocol** -- Add or remove a UDP server address for the VLAN **(p. 473)**
    - **udp** -- Add or remove a UDP server address for the VLAN **(p. 492)**
      - **ip-addr** -- IP address of the protocol server. (IP-ADDR) **(p. 476)**
        - **port-name < dns | ntp | netbios-ns | ... >** -- (NUMBER) **(p. 486)**
        - **port-num** -- UDP port number of the server. (TCP/UDP-PORT) **(p. 486)**

© 2007 Hewlett-Packard Development Company, L.P.

- **helper-address** -- Add or remove a DHCP server IP address for the VLAN (IP-ADDR) **(p. 474)**
- **igmp** -- Enable/disable/configure IP Multicast Group Protocol (IGMP) feature on a VLAN **(p. 475)**
  - **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 469)**
  - **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 470)**
  - **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 472)**
  - **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 472)**
  - **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 472)**
  - **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups **(p. 474)**
  - **querier** -- Specify querier/non-querier capability for the VLAN **(p. 489)**
- **irdp** -- Configure ICMP Router Discovery Protocol (IRDP) **(p. 478)**
  - **advert-address < multicast | broadcast >** -- Specify the destination address to be used for router advertisements **(p. 465)**
  - **holdtime < 4 to 9000 >** -- Set the lifetime (in seconds) of the router advertisements sent on this interface **(p. 474)**
  - **maxadvertinterval < 4 to 1800 >** -- Set the maximum time (in seconds) allowed between sending unsolicited router advertisements **(p. 480)**
  - **minadvertinterval < 3 to 1800 >** -- Set the minimum time (in seconds) allowed between sending unsolicited router advertisements **(p. 481)**
  - **preference** -- The preferability of the router as a default router, relative to the other routers on the same subnet **(p. 486)**
    - **no-default** -- Indicates that the router should never be used as a default by its neighbors. **(p. 483)**
    - **number < -2147483647 to 2147483647 >** -- The router preferability number. Higher values are more preferable. **(p. 483)**
- **mroute** -- Configure IP Multicast Routing parameters on the VLAN interface **(p. 482)**
  - **ttl-threshold < 0 to 255 >** -- Set the multicast datagram TTL threshold for the interface **(p. 492)**
- **ospf** -- Enable/disable/configure Open Shortest Path First (OSPF) protocol on the VLAN interface **(p. 483)**
  - **all** -- Process the request for all IP addresses. **(p. 465)**
    - **area** -- Specify an OSPF area. **(p. 466)**
      - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 467)**
      - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 469)**
    - **authentication** -- Disable authentication. **(p. 467)**
    - **authentication-key** -- Set simple authentication method and key. **(p. 467)**
      - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 467)**
    - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 470)**
    - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 471)**
    - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 473)**
    - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 480)**
      - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 470)**
    - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 487)**
    - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 490)**
    - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 492)**
  - **area** -- Specify an OSPF area. **(p. 466)**
    - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 467)**

© 2007 Hewlett-Packard Development Company, L.P.

        - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 469)**
    - **authentication** -- Disable authentication. **(p. 467)**
    - **authentication-key** -- Set simple authentication method and key. **(p. 467)**
        - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 467)**
    - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 470)**
    - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 471)**
    - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 473)**
    - **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 476)**
        - **area** -- Specify an OSPF area. **(p. 466)**
            - **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 467)**
            - **backbone** -- The backbone area (the same as 0.0.0.0). **(p. 469)**
        - **authentication** -- Disable authentication. **(p. 467)**
        - **authentication-key** -- Set simple authentication method and key. **(p. 467)**
            - **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 467)**
        - **cost < 1 to 65535 >** -- Set metric of this interface. **(p. 470)**
        - **dead-interval < 1 to 65535 >** -- Set dead interval in seconds; the default is 40. **(p. 471)**
        - **hello-interval < 1 to 65535 >** -- Set hello interval in seconds; the default is 10. **(p. 473)**
        - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 480)**
            - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 470)**
        - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 487)**
        - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 490)**
        - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 492)**
    - **md5-auth-key-chain** -- Set MD5 authentication method and key chain. **(p. 480)**
        - **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 470)**
    - **priority < 0 to 255 >** -- Set priority of this router as a designated router. **(p. 487)**
    - **retransmit-interval < 1 to 3600 >** -- Set retransmit interval in seconds; the default is 5. **(p. 490)**
    - **transit-delay < 1 to 3600 >** -- Set transit delay in seconds; the default is 1. **(p. 492)**
- **pim-dense** -- Enable/disable/configure PIM-DM protocol on the VLAN interface **(p. 484)**
    - **graft-retry-interval < 1 to 10 >** -- Set the interval a PIM router waits for a Graft Ack before resending a Graft on this interface **(p. 473)**
    - **hello-delay < 0 to 5 >** -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface **(p. 473)**
    - **hello-interval < 5 to 300 >** -- Set the frequency at which PIM Hello messages are transmitted on this interface **(p. 473)**
    - **ip-addr** -- Set the source IP address for the PIM-DM packets sent out on this interface **(p. 476)**
        - **any** -- Dynamically determine IP address. **(p. 466)**
        - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 476)**
    - **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface **(p. 479)**
    - **max-graft-retries < 1 to 10 >** -- Set the maximum number of times this router will resend a Graft on this interface **(p. 480)**
    - **override-interval < 500 to 6000 >** -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface **(p. 484)**
    - **propagation-delay < 250 to 2000 >** -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface **(p. 487)**
    - **ttl-threshold < 0 to 255 >** -- Set the Time To Live in a PIM-DM State Refresh message at which it is not forwarded on this interface **(p. 492)**
- **pim-sparse** -- Enable/disable/configure PIM-SM protocol on the VLAN interface **(p. 485)**

© 2007 Hewlett-Packard Development Company, L.P.

- **dr-priority** -- Set the priority value to use on the interface in the Designated Router election process **(p. 471)**
- **hello-delay < 0 to 5 >** -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface **(p. 473)**
- **hello-interval < 5 to 300 >** -- Set the frequency at which PIM Hello messages are transmitted on this interface **(p. 473)**
- **ip-addr** -- Set the source IP address for the PIM-SM packets sent out on this interface **(p. 476)**
  - **any** -- Dynamically determine IP address. **(p. 466)**
  - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 476)**
- **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface **(p. 479)**
- **nbr-timeout < 60 to 8000 >** -- Set the neighbour loss time interval for this interface **(p. 483)**
- **override-interval < 500 to 6000 >** -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface **(p. 484)**
- **propagation-delay < 250 to 2000 >** -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface **(p. 487)**

- **proxy-arp** -- Enable/disable proxy ARP **(p. 488)**
- **rip** -- Enable/disable/configure Routing Internet Protocol (RIP) on the VLAN interface **(p. 490)**
  - **all** -- Process the request for all IP addresses. **(p. 465)**
    - **authentication-key** -- Set authentication key. **(p. 467)**
      - **auth-key-text** -- Set authentication key. (OCTET-STR) **(p. 469)**
    - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 468)**
    - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 480)**
    - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 485)**
    - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 489)**
    - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 490)**
    - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 491)**
  - **authentication-key** -- Set authentication key. **(p. 467)**
    - **auth-key-text** -- Set authentication key. (OCTET-STR) **(p. 469)**
  - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 468)**
  - **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 476)**
    - **authentication-key** -- Set authentication key. **(p. 467)**
      - **auth-key-text** -- Set authentication key. (OCTET-STR) **(p. 469)**
    - **authentication-type < none | text >** -- Set authentication type used on this interface. **(p. 468)**
    - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 480)**
    - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 485)**
    - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 489)**
    - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 490)**
    - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 491)**
  - **metric < 1 to 15 >** -- Set metric for this interface. **(p. 480)**
  - **poison-reverse** -- Enable/disable poison reverse on this interface. **(p. 485)**
  - **receive < V1-only | V2-only | V1-or-V2 | ... >** -- Define RIP version for incoming packets. **(p. 489)**
  - **rip-compatible < V1-only | V2-only | V1-or-V2 >** -- Define RIP version for incoming and outgoing packets. **(p. 490)**

© 2007 Hewlett-Packard Development Company, L.P.

        - **send < disabled | V1-only | V1-compatible-V2 | ... >** -- Define RIP version for outgoing packets. **(p. 491)**
- [no] vlan VLAN-ID **ip-recv-mac-address** -- Associates a L3-mac-address with a VLAN **(p. 478)**
  - **mac-address** -- The L3-mac-address to be associated with a VLAN. (MAC-ADDR) **(p. 479)**
    - **interval** -- Specify the L3-Mac-Address timeout interval. **(p. 475)**
      - **timer-interval < 1 to 255 >** -- Timeout interval in seconds <1-255>. **(p. 492)**
- [no] vlan VLAN-ID **jumbo** -- Labels this VLAN as a Jumbo VLAN, allowing you to pass packets up to 9220 bytes in size **(p. 479)**
- [no] vlan VLAN-ID **monitor** -- Define either the VLAN is to be monitored or not **(p. 481)**
  - **all < In | Out | Both >** -- Monitor all traffic. **(p. 465)**
    - **mirror** -- Mirror destination. **(p. 481)**
      - **mirror_session_name** -- Mirror destination name. **(p. 481)**
      - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 482)**
  - **ip** -- Apply an IPv4 access list. **(p. 476)**
    - **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 463)**
      - **monitor_mirror_ACL_dir < In >** -- Define the mirror port for diagnostic purposes **(p. 482)**
        - **mirror** -- Mirror destination. **(p. 481)**
          - **mirror_session_name** -- Mirror destination name. **(p. 481)**
          - **monitor_mirror_session_id < 1 to 4 >** -- Mirror destination number. **(p. 482)**
- vlan VLAN-ID **name** -- Set the VLAN's name (ASCII-STR) **(p. 483)**
- [no] vlan VLAN-ID **protocol** -- Set a predefined protocol for the current VLAN. **(p. 488)**
  - **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 488)**
  - **protocols < IPX | IPv4 | IPv6 | ... >** -- Set a predefined protocol for the current VLAN. **(p. 488)**
- [no] vlan VLAN-ID **qos** -- Set VLAN-based priority **(p. 489)**
  - **dscp < 000000 | 000001 | 000010 | ... >** -- Specify DSCP policy to use. **(p. 471)**
  - **priority < 0 | 1 | 2 | ... >** -- Specify priority to use. **(p. 487)**
- [no] vlan VLAN-ID **tagged** -- Assign ports to current VLAN as tagged ([ethernet] PORT-LIST) **(p. 492)**
- [no] vlan VLAN-ID **untagged** -- Assign ports to current VLAN as untagged ([ethernet] PORT-LIST) **(p. 493)**
- [no] vlan VLAN-ID **voice** -- Labels this VLAN as a Voice VLAN, allowing you to separate, prioritize, and authenticate voice traffic moving through your network **(p. 493)**
- [no] vlan VLAN-ID **vrrp** -- Enable/disable/configure VRRP operation on the VLAN **(p. 494)**
  - **vrid < 1 to 255 >** -- Configure a virtual router instance for the VLAN **(p. 494)**
    - **advertise-interval < 1 to 255 >** -- Set time interval (in seconds) between sending VRRP advertisement messages **(p. 465)**
    - **backup** -- Designate the virtual router instance as a Backup **(p. 469)**
    - **enable** -- Enable/disable operation of the virtual router instance **(p. 472)**
    - **owner** -- Designate the virtual router instance as an Owner (Master) **(p. 484)**
    - **preempt-mode** -- Enable/disable preempt mode for the virtual router instance **(p. 486)**
    - **primary-ip-address** -- Specify IP address the virtual router instance will use as a source in VRRP advertisement messages **(p. 487)**
      - **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 476)**
      - **lowest** -- Dynamically determine lowest IP address. **(p. 479)**
    - **priority < 1 to 255 >** -- Configure priority for the virtual router instance **(p. 487)**
    - **virtual-ip-address** -- Specify IP address to be supported by the virtual router instance **(p. 493)**
      - **ip-addr** -- Specify IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 476)**

© 2007 Hewlett-Packard Development Company, L.P.

EXAMPLES

Example: vlan name

Change VLAN 100's name to "Blue_Team" and add ports A1 - A5 as tagged members of the VLAN:

```
ProCurve(config)# vlan 100 name Blue_Team
ProCurve(config)# vlan 100 tagged a1-a5
```

Example: vlan default_vlan

Go to a different VLAN context level, such as to the default VLAN:

```
ProCurve(vlan-100)# vlan default_vlan
```

Example: vlan ip address

Configure IP addressing on the default VLAN with the subnet mask specified in mask bits:

```
ProCurve(config)# vlan 1 ip address 10.28.227.103 255.255.255.0
```

Example: vlan ip address

Configure the same IP addressing as the preceding example, but specify the subnet mask by mask length:

```
ProCurve(config)# vlan 1 ip address 10.28.227.103/24
```

Example: vlan ip address

Delete an IP address configured in VLAN 1:

```
ProCurve(config) no vlan 1 ip address 10.28.227.103/24
```

Example: vlan ip igmp

Configure IGMP on VLAN 1:

```
ProCurve(config)# vlan 1 ip igmp auto a1,a2 forward a3,a4 blocked a5,a6
ProCurve(config)# ip igmp auto a1,a2 forward a3,a4 blocked a5,a6
```

Example: vlan ip igmp high-priority-forward

Configure high priority for IGMP traffic on VLAN 1:

```
ProCurve(config)# vlan 1 ip igmp high-priority-forward
```

Example: vlan ip igmp high-priority-forward

Same as above command, but in the VLAN 1 context level:

```
ProCurve(vlan-1)# ip igmp high-priority-forward
```

Example: vlan ip igmp high-priority-forward

Return IGMP traffic to "normal" priority:

```
ProCurve(vlan 1)# no ip igmp high-priority-forward
```

© 2007 Hewlett-Packard Development Company, L.P.

Example: vlan tagged

Change the tagged ports in the above examples to No (or Auto, if GVRP is enabled):

```
ProCurve(config)# no vlan 100 tagged a1-a5
```

Example: vlan tagged

Configure a voice VLAN with a VID of 10, and set the highest priority for all traffic on this VLAN:

```
ProCurve(config)# vlan 10 qos priority 7
ProCurve(config)# write memory
```

COMMAND DETAILS

access-group (p. 463)
address (p. 464)
advert-address (p. 465)
advertise-interval (p. 465)
all (p. 465)
any (p. 466)
area (p. 466)
area-id (p. 467)
authentication (p. 467)
authentication-key (p. 467)
authentication-type (p. 468)
auth-key-text (p. 469)
auto (p. 469)
backbone (p. 469)
backup (p. 469)
blocked (p. 470)
chain-name (p. 470)
connection-rate-filter (p. 470)
cost (p. 470)
dead-interval (p. 471)
dhcp-bootp (p. 471)
dhcp-snooping (p. 471)
direction (p. 471)
domain-name (p. 471)
dr-priority (p. 471)
dscp (p. 471)
enable (p. 472)
fastleave (p. 472)
forbid (p. 472)
forcedfastleave (p. 472)
forward (p. 472)
forward-protocol (p. 473)
graft-retry-interval (p. 473)
hello-delay (p. 473)
hello-interval (p. 473)
helper-address (p. 474)
high-priority-forward (p. 474)
holdtime (p. 474)
host (p. 474)
igmp (p. 475)
igmp-proxy (p. 475)
interval (p. 475)
ip (p. 476)
ip-addr (p. 476)
ip-recv-mac-address (p. 478)
irdp (p. 478)
jumbo (p. 479)
lan-prune-delay (p. 479)
lowest (p. 479)
mac-address (p. 479)
maxadvertinterval (p. 480)
max-graft-retries (p. 480)
md5-auth-key-chain (p. 480)
metric (p. 480)
minadvertinterval (p. 481)
mirror (p. 481)
mirror_session_name (p. 481)
monitor (p. 481)
monitor_mirror_ACL_dir (p. 482)
monitor_mirror_session_id (p. 482)
mroute (p. 482)
name (p. 483)
nbr-timeout (p. 483)
no-default (p. 483)
number (p. 483)
ospf (p. 483)
override-interval (p. 484)
owner (p. 484)
pim-dense (p. 484)
pim-sparse (p. 485)
poison-reverse (p. 485)
port-name (p. 486)
port-num (p. 486)
preempt-mode (p. 486)
preference (p. 486)
primary-ip-address (p. 487)
priority (p. 487)
propagation-delay (p. 487)
protocol (p. 488)
protocol-group (p. 488)
protocols (p. 488)
proxy-arp (p. 488)
qos (p. 489)
querier (p. 489)
receive (p. 489)
retransmit-interval (p. 490)
rip (p. 490)
rip-compatible (p. 490)
send (p. 491)
src-ip (p. 491)
tagged (p. 492)
timer-interval (p. 492)
transit-delay (p. 492)
ttl-threshold (p. 492)
udp (p. 492)
unblock (p. 493)
untagged (p. 493)
virtual-ip-address (p. 493)
voice (p. 493)
vrid (p. 494)
vrrp (p. 494)

access-group

- [no] vlan *VLAN-ID* ip access-group *ACCESS-GROUP*

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] ip access-group <ACL-ID> <in|out>

Description: Apply the specified access control list to either inbound
             or outbound packets on this VLAN interface.  The access
             control list ACL-ID must be defined before it can be applied.
```

Next Available Option:

- **direction** < in | out | connection-rate-filter | ... > -- **(p. 471)**

■ vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Next Available Option:

- **monitor_mirror_ACL_dir** < In > -- Define the mirror port for diagnostic purposes**(p. 482)**

address

■ [no] vlan *VLAN-ID* ip address

```
Usage: [no] ip address [dhcp-bootp|IP-ADDR/MASK-LENGTH]

Description: Set IP parameters for communication within an IP network.
             Each VLAN represents an IP interface having its own unique
             configuration.  The VLAN for which the configuration is
             applied can be specified implicitly by preceding the
             phrase 'ip address' with the 'vlan VLAN-ID' keyword and
             argument.  It can also be called explicitly when called
             directly from a VLAN context.  In the latter case the
             command affects the VLAN identified by the context.

Parameters:

    o dhcp-bootp - The switch attempts to get its configuration from a
      DHCP/Bootp server.

    o IP-ADDR/MASK-LENGTH - Assign an IP address to the switch or VLAN.
      The IP-ADDR/MASK-LENGTH may be specified in two ways using the
      following syntax:
          ip address 192.32.36.87/24
          ip address 192.32.36.87 255.255.255.0
      Both of the statements above would have the same effect.
      Multiple addresses may be configured on a single VLAN.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:
- **ip-addr** -- Interface IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 476)**
- **dhcp-bootp** -- Configure the interface to use DHCP/Bootp server to acquire parameters.**(p. 471)**

advert-address

- vlan *VLAN-ID* ip irdp *< multicast | broadcast >*

```
Usage: [no] ip irdp <multicast|broadcast>

Description: Specify the destination address to be used for router
             advertisements.
             It has to be either multicast or broadcast. If the value
             of this object is 'multicast' (the default), router
             advertisements will be sent to the all-hosts multicast
             address, 224.0.0.1. If the value of this object is 'broadcast',
             router advertisements sent on this interface will be sent to
             the limitied broadcast address, 255.255.255.255.
```

Supported Values:
- **multicast** -- Send advertisements to all-hosts multicast address.
- **broadcast** -- Send advertisements to broadcast address.

advertise-interval

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* advertise-interval *< 1 to 255 >*

```
Usage: vrrp vrid <VRID> advertise-interval <1-255>

Description: Set time interval (in seconds) between sending VRRP advertisement
             messages. The default value is one second.
```

Range: < 1 to 255 >

all

- [no] vlan *VLAN-ID* ip ospf all

```
Process the request for all IP addresses.
```

Next Available Options:
- **area** -- Specify an OSPF area.**(p. 466)**
- **authentication-key** -- Set simple authentication method and key.**(p. 467)**
- **authentication** -- Disable authentication.**(p. 467)**
- **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 480)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 470)**
- **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 471)**
- **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 473)**
- **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 487)**
- **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 490)**
- **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 492)**

- [no] vlan *VLAN-ID* ip rip all

```
Process the request for all IP addresses.
```

Next Available Options:

© 2007 Hewlett-Packard Development Company, L.P.

- **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 468)**
- **authentication-key** -- Set authentication key.**(p. 467)**
- **metric** < 1 to 15 > -- Set metric for this interface.**(p. 480)**
- **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 485)**
- **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 489)**
- **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 491)**
- **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 490)**

■ vlan *VLAN-ID* connection-rate-filter unblock all

```
Resets all previously blocked by the connection rate filter
```

■ vlan *VLAN-ID* monitor all *< In | Out | Both >*

```
Monitor all traffic.
```

Supported Values:
- **In** -- Monitor all inbound traffic
- **Out** -- Monitor all outbound traffic
- **Both** -- Monitor all inbound and outbound traffic

Next Available Option:
- **mirror** -- Mirror destination.**(p. 481)**

any

■ vlan *VLAN-ID* ip pim-dense ip-addr any

```
Dynamically determine IP address.
```

■ vlan *VLAN-ID* ip pim-sparse ip-addr any

```
Dynamically determine IP address.
```

area

■ vlan *VLAN-ID* ip ospf area

```
Specify an OSPF area.
```

Next Available Options:
- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 467)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 469)**

■ vlan *VLAN-ID* ip ospf *IP-ADDR* area

```
Specify an OSPF area.
```

Next Available Options:
- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 467)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 469)**

© 2007 Hewlett-Packard Development Company, L.P.

- vlan *VLAN-ID* ip ospf all area

```
Specify an OSPF area.
```

Next Available Options:
- **area-id** -- Single integer or IP address style dotted decimal. (OSPF-AREA-ID) **(p. 467)**
- **backbone** -- The backbone area (the same as 0.0.0.0).**(p. 469)**

area-id

- vlan *VLAN-ID* ip ospf area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

- vlan *VLAN-ID* ip ospf *IP-ADDR* area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

- vlan *VLAN-ID* ip ospf all area *OSPF-AREA-ID*

```
Single integer or IP address style dotted decimal.
```

authentication

- [no] vlan *VLAN-ID* ip ospf authentication

```
Disable authentication.
```

- [no] vlan *VLAN-ID* ip ospf *IP-ADDR* authentication

```
Disable authentication.
```

- [no] vlan *VLAN-ID* ip ospf all authentication

```
Disable authentication.
```

authentication-key

- vlan *VLAN-ID* ip ospf authentication-key

```
Set simple authentication method and key.
```

Next Available Option:
- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 467)**

- vlan *VLAN-ID* ip ospf authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

- vlan *VLAN-ID* ip ospf *IP-ADDR* authentication-key

```
Set simple authentication method and key.
```

Next Available Option:
- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 467)**

- vlan *VLAN-ID* ip ospf *IP-ADDR* authentication-key *OCTET-STR*

© 2007 Hewlett-Packard Development Company, L.P.

```
OSPF authentication key (maximum 8 characters).
```

- vlan *VLAN-ID* ip ospf all authentication-key

```
Set simple authentication method and key.
```

Next Available Option:
- **authentication-key** -- OSPF authentication key (maximum 8 characters). (OCTET-STR) **(p. 467)**

- vlan *VLAN-ID* ip ospf all authentication-key *OCTET-STR*

```
OSPF authentication key (maximum 8 characters).
```

- [no] vlan *VLAN-ID* ip rip authentication-key

```
Set authentication key.
```

Next Available Option:
- **auth-key-text** -- Set authentication key. (OCTET-STR) **(p. 469)**

- [no] vlan *VLAN-ID* ip rip *IP-ADDR* authentication-key

```
Set authentication key.
```

Next Available Option:
- **auth-key-text** -- Set authentication key. (OCTET-STR) **(p. 469)**

- [no] vlan *VLAN-ID* ip rip all authentication-key

```
Set authentication key.
```

Next Available Option:
- **auth-key-text** -- Set authentication key. (OCTET-STR) **(p. 469)**

authentication-type

- vlan *VLAN-ID* ip rip authentication-type *< none | text >*

```
Set authentication type used on this interface.
```

Supported Values:
- **none** -- Do not use authentication.
- **text** -- Use simple password.

- vlan *VLAN-ID* ip rip *IP-ADDR* authentication-type *< none | text >*

```
Set authentication type used on this interface.
```

Supported Values:
- **none** -- Do not use authentication.
- **text** -- Use simple password.

- vlan *VLAN-ID* ip rip all authentication-type *< none | text >*

```
Set authentication type used on this interface.
```

Supported Values:

© 2007 Hewlett-Packard Development Company, L.P.

- **none** -- Do not use authentication.
- **text** -- Use simple password.

auth-key-text

- vlan *VLAN-ID* ip rip authentication-key *OCTET-STR*

```
Set authentication key.
```

- vlan *VLAN-ID* ip rip *IP-ADDR* authentication-key *OCTET-STR*

```
Set authentication key.
```

- vlan *VLAN-ID* ip rip all authentication-key *OCTET-STR*

```
Set authentication key.
```

auto

- vlan *VLAN-ID* auto *[ETHERNET] PORT-LIST*

```
Usage: [no] auto [ethernet] PORT-LIST

Description: Cause each port identified in the port list to learn its
             VLAN membership using the GARP VLAN Registration Protocol
             (GVRP). This command is only valid when GVRP is enabled.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

- vlan *VLAN-ID* ip igmp auto *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp auto [ethernet] PORT-LIST

Description: Instruct the device to monitor incoming multicast traffic
             on the specified ports (this is the default behavior).  This
             feature is configured on a per-VLAN basis.
```

backbone

- vlan *VLAN-ID* ip ospf area backbone

```
The backbone area (the same as 0.0.0.0).
```

- vlan *VLAN-ID* ip ospf *IP-ADDR* area backbone

```
The backbone area (the same as 0.0.0.0).
```

- vlan *VLAN-ID* ip ospf all area backbone

```
The backbone area (the same as 0.0.0.0).
```

backup

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* backup

```
Usage: vrrp vrid <VRID> backup

Description: Designate the virtual router instance as a Backup.
             There is no default value.
```

© 2007 Hewlett-Packard Development Company, L.P.

blocked

- vlan *VLAN-ID* ip igmp blocked *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp block [ethernet] PORT-LIST

Description: Instruct the device to drop incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

chain-name

- vlan *VLAN-ID* ip ospf md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

- vlan *VLAN-ID* ip ospf *IP-ADDR* md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

- vlan *VLAN-ID* ip ospf all md5-auth-key-chain *CHAIN-NAME*

```
Specify key chain to use for MD5 authentication.
```

connection-rate-filter

- vlan *VLAN-ID* connection-rate-filter

```
Usage:      connection-rate-filter unblock < host SRC-IP-ADDR | SRC-IP-ADDRESS/MASK
>
       [no] connection-rate-filter sensitivity <low|medium|high|aggressive>

Description: Re-enables access to a host or set of hosts  that has been previously
             blocked by the connection rate filter. Disabling or setting sensitivity

             may have improved performance after rebooting the switch
```

Next Available Option:

- **unblock** -- Resets a host previously blocked by the connection rate filter **(p. 493)**

cost

- vlan *VLAN-ID* ip ospf cost *< 1 to 65535 >*

```
Set metric of this interface.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* cost *< 1 to 65535 >*

```
Set metric of this interface.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip ospf all cost *< 1 to 65535 >*

```
Set metric of this interface.
```

Range: < 1 to 65535 >

© 2007 Hewlett-Packard Development Company, L.P.

dead-interval

- vlan *VLAN-ID* ip ospf dead-interval *< 1 to 65535 >*

```
Set dead interval in seconds; the default is 40.
```

  Range: < 1 to 65535 >
- vlan *VLAN-ID* ip ospf *IP-ADDR* dead-interval *< 1 to 65535 >*

```
Set dead interval in seconds; the default is 40.
```

  Range: < 1 to 65535 >
- vlan *VLAN-ID* ip ospf all dead-interval *< 1 to 65535 >*

```
Set dead interval in seconds; the default is 40.
```

  Range: < 1 to 65535 >

dhcp-bootp

- vlan *VLAN-ID* ip address dhcp-bootp

```
Configure the interface to use DHCP/Bootp server to acquire parameters.
```

dhcp-snooping

- [no] vlan *VLAN-ID* dhcp-snooping

direction

- [no] vlan *VLAN-ID* ip access-group *ACCESS-GROUP < in | out | connection-rate-filter | ... >*

  Supported Values:
  - **in** -- Match inbound packets
  - **out** -- Match outbound packets
  - **connection-rate-filter** -- Manage packet rates
  - **vlan** -- VLAN acl

domain-name

- [no] vlan *VLAN-ID* igmp-proxy *<DOMAIN-NAME>*

```
Specify the domain name to associate/disassociate with the VLAN.
```

dr-priority

- vlan *VLAN-ID* ip pim-sparse dr-priority *INTEGER*

```
Usage: ip pim-sparse dr-priority <0-2147483647>

Description: Set the priority value to use on the interface in the Designated
             Router election process. Default is 1.
```

dscp

- vlan *VLAN-ID* qos dscp *< 000000 | 000001 | 000010 | ... >*

```
Specify DSCP policy to use.
```

  Supported Values:

  Binary formatted value from 000000 to 111111

© 2007 Hewlett-Packard Development Company, L.P.

enable

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* enable

```
Usage: [no] vrrp vrid <VRID> enable

Description: Enable/disable operation of the virtual router instance.
             The default value is 'disabled'.
```

fastleave

- [no] vlan *VLAN-ID* ip igmp fastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp fastleave [ethernet] PORT-LIST

Description: Enables or disables IGMP Fast Leaves. When enabled, as soon as
             an IGMP Group Leave has been received on a non-cascaded port,
             the switch stops forwarding multicast traffic for that group
             to that port.
             Does not apply to cascaded ports (see ip igmp forcedfastleave).
             When disabled, or when the port is cascaded, the regular IGMP
             leave time is used (up to 10 seconds when the switch is not
             the IGMP Querier).
             The default behavior is for IGMP FastLeaves to be enabled.
             This feature is configured for ports on a per-VLAN basis.
```

forbid

- [no] vlan *VLAN-ID* forbid *[ETHERNET] PORT-LIST*

```
Usage: [no] forbid [ethernet] PORT-LIST

Description: Prevent ports from becoming a member of the current VLAN.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

forcedfastleave

- [no] vlan *VLAN-ID* ip igmp forcedfastleave *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp forcedfastleave [ethernet] PORT-LIST

Description: When enabled, this feature forces IGMP Fast Leaves to occur
             even when the port is cascaded. See 'ip igmp fastleave' for
             more information.  The default behavior is for IGMP Forced
             FastLeaves to be disabled.
             This feature is configured for ports on a per-VLAN basis.
```

forward

- vlan *VLAN-ID* ip igmp forward *[ETHERNET] PORT-LIST*

```
Usage: [no] ip igmp forward [ethernet] PORT-LIST

Description: Instruct the device to forward incoming multicast packets
             received on the specified ports.  This feature is
             configured on a per-VLAN basis.
```

© 2007 Hewlett-Packard Development Company, L.P.

forward-protocol

- vlan *VLAN-ID* ip forward-protocol

```
Usage: [no] ip forward-protocol udp IP-ADDR PORT-NUM|PORT-NAME

Description: Add or remove a UDP server address for the VLAN. The
             broadcast  packets received by the switch on this VLAN are to
             be forwarded to the specified application server.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Option:

- **udp** -- Add or remove a UDP server address for the VLAN**(p. 492)**

graft-retry-interval

- vlan *VLAN-ID* ip pim-dense graft-retry-interval *< 1 to 10 >*

```
Usage: ip pim-dense graft-retry-interval <1-10>

Description: Set the interval a PIM router waits for a Graft Ack before
             resending a Graft on this interface. Default value is 3
             seconds.
```

Range: < 1 to 10 >

hello-delay

- vlan *VLAN-ID* ip pim-dense hello-delay *< 0 to 5 >*

```
Usage: ip pim-dense hello-delay <0-5>

Description: Set the maximum time before a triggered PIM Hello message is
             transmitted on this interface. Default value is 5 seconds.
```

Range: < 0 to 5 >

- vlan *VLAN-ID* ip pim-sparse hello-delay *< 0 to 5 >*

```
Usage: ip pim-sparse hello-delay <0-5>

Description: Set the maximum time before a triggered PIM Hello message is
             transmitted on this interface. Default value is 5 seconds.
```

Range: < 0 to 5 >

hello-interval

- vlan *VLAN-ID* ip ospf hello-interval *< 1 to 65535 >*

```
Set hello interval in seconds; the default is 10.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* hello-interval *< 1 to 65535 >*

```
Set hello interval in seconds; the default is 10.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip ospf all hello-interval *< 1 to 65535 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Set hello interval in seconds; the default is 10.
```

Range: < 1 to 65535 >

- vlan *VLAN-ID* ip pim-dense hello-interval *< 5 to 300 >*

```
Usage: ip pim-dense hello-interval <5-300>

Description: Set the frequency at which PIM Hello messages are transmitted
             on this interface. Default value is 30 seconds.
```

Range: < 5 to 300 >

- vlan *VLAN-ID* ip pim-sparse hello-interval *< 5 to 300 >*

```
Usage: ip pim-sparse hello-interval <5-300>

Description: Set the frequency at which PIM Hello messages are transmitted
             on this interface. Default value is 30 seconds.
```

Range: < 5 to 300 >

helper-address

- [no] vlan *VLAN-ID* ip helper-address *IP-ADDR*

```
Usage: [no] ip helper-address IP-ADDR

Description: Add or remove a DHCP server IP address for the VLAN. The
             DHCP requests received by the switch on this VLAN are to
             be relayed to the specified DHCP server.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

high-priority-forward

- [no] vlan *VLAN-ID* ip igmp high-priority-forward

```
Usage: [no] ip igmp high-priority-forward

Description: Enable/disable the high priority forwarding of traffic for
             subscribed IP Multicast groups. This feature is configured on
             a per-VLAN  basis.
```

holdtime

- vlan *VLAN-ID* ip irdp holdtime *< 4 to 9000 >*

```
Usage: [no] ip irdp holdtime <4-9000>

Description: Set the lifetime (in seconds) of the router advertisements sent
             on this interface. Must be no less than the maximum time
             allowed between sending unsolicited router advertisements.
```

Range: < 4 to 9000 >

host

- vlan *VLAN-ID* connection-rate-filter unblock host *IP-ADDR*

```
Match packets from the specified IP address.
```

© 2007 Hewlett-Packard Development Company, L.P.

igmp

- [no] vlan *VLAN-ID* ip igmp

```
Usage: [no] ip igmp [...]

Description: Enable/disable/configure IP Multicast Group Protocol (IGMP)
             feature on a VLAN.  This command enables, disables or
             configures the IGMP feature for IGMP communication between
             Multicast Routers, Multicast Servers, and Multicast Clients
             connected to the device.  This is a VLAN context command. It
             can be called directly from the VLAN context or may follow
             the 'vlan VLAN-ID' command prefix.  If not preceded by 'no',
             the command accepts a variety of configuration parameters. To
             get a list of all available parameters use 'ip igmp ?'. To
             get detailed help for a parameter follow it with 'help'
             keyword.
```

Next Available Options:

- **querier** -- Specify querier/non-querier capability for the VLAN**(p. 489)**
- **high-priority-forward** -- Enable/disable the high priority forwarding of traffic for subscribed IP Multicast groups**(p. 474)**
- **auto** -- Instruct the device to monitor incoming multicast traffic on the specified ports (this is the default behavior) ([ethernet] PORT-LIST) **(p. 469)**
- **blocked** -- Instruct the device to drop incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 470)**
- **fastleave** -- Enables or disables IGMP Fast Leaves ([ethernet] PORT-LIST) **(p. 472)**
- **forcedfastleave** -- When enabled, this feature forces IGMP Fast Leaves to occur even when the port is cascaded ([ethernet] PORT-LIST) **(p. 472)**
- **forward** -- Instruct the device to forward incoming multicast packets received on the specified ports ([ethernet] PORT-LIST) **(p. 472)**

igmp-proxy

- [no] vlan *VLAN-ID* igmp-proxy

```
Usage: [no] igmp-proxy DOMAIN-NAME

Description: Associate an IGMP proxy domain with a VLAN.
             If the 'no' keyword is used:
                 If the DOMAIN-NAME is left blank, all the domains
                 associated with the respective VLAN will be disassociated.
                 If a DOMAIN-NAME is specified, The specified domain will
                 be disassociated from the respecive VLAN.
             If the 'no' keyword is not used:
                 If the DOMAIN-NAME matches the domain name of an
                 existing domain, the respective domain will be associated
                 with the respective VLAN.
```

Next Available Option:

- **domain-name** < DOMAIN-NAME > -- Specify the domain name to associate/disassociate with the VLAN. (ASCII-STR) **(p. 471)**

interval

- vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR* interval

```
Specify the L3-Mac-Address timeout interval.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Option:
- **timer-interval** < 1 to 255 > -- Timeout interval in seconds <1-255>. **(p. 492)**

ip

- vlan *VLAN-ID* ip

```
Usage: [no] ip ...

Description: Configure various IP parameters for the VLAN. The 'ip'
             command must be followed by a feature-specific keyword.
             Use 'ip ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:
- **access-group** -- Apply the specified access control list to either inbound or outbound packets on this VLAN interface (ASCII-STR) **(p. 463)**
- **address** -- Set IP parameters for communication within an IP network**(p. 464)**
- **helper-address** -- Add or remove a DHCP server IP address for the VLAN (IP-ADDR) **(p. 474)**
- **forward-protocol** -- Add or remove a UDP server address for the VLAN**(p. 473)**
- **igmp** -- Enable/disable/configure IP Multicast Group Protocol (IGMP) feature on a VLAN**(p. 475)**
- **irdp** -- Configure ICMP Router Discovery Protocol (IRDP)**(p. 478)**
- **proxy-arp** -- Enable/disable proxy ARP**(p. 488)**
- **ospf** -- Enable/disable/configure Open Shortest Path First (OSPF) protocol on the VLAN interface**(p. 483)**
- **rip** -- Enable/disable/configure Routing Internet Protocol (RIP) on the VLAN interface**(p. 490)**
- **pim-dense** -- Enable/disable/configure PIM-DM protocol on the VLAN interface**(p. 484)**
- **pim-sparse** -- Enable/disable/configure PIM-SM protocol on the VLAN interface**(p. 485)**
- **mroute** -- Configure IP Multicast Routing parameters on the VLAN interface**(p. 482)**

- [no] vlan *VLAN-ID* monitor ip

```
Apply an IPv4 access list.
```

Next Available Option:
- **access-group** -- Define the mirror port for diagnostic purposes (ASCII-STR) **(p. 463)**

ip-addr

- [no] vlan *VLAN-ID* ip address *IP-ADDR/MASK-LENGTH*

```
Interface IP address/mask.
```

- [no] vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR*

```
IP address of the protocol server.
```

Next Available Options:
- **port-num** -- UDP port number of the server. (TCP/UDP-PORT) **(p. 486)**
- **port-name** < dns | ntp | netbios-ns | ... > -- (NUMBER) **(p. 486)**

© 2007 Hewlett-Packard Development Company, L.P.

- [no] vlan *VLAN-ID* ip ospf *IP-ADDR*

```
Specify the IP address the request is for.
```

Next Available Options:
- **area** -- Specify an OSPF area.**(p. 466)**
- **authentication-key** -- Set simple authentication method and key.**(p. 467)**
- **authentication** -- Disable authentication.**(p. 467)**
- **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 480)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 470)**
- **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 471)**
- **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 473)**
- **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 487)**
- **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 490)**
- **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 492)**

- [no] vlan *VLAN-ID* ip rip *IP-ADDR*

```
Specify the IP address the request is for.
```

Next Available Options:
- **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 468)**
- **authentication-key** -- Set authentication key.**(p. 467)**
- **metric** < 1 to 15 > -- Set metric for this interface.**(p. 480)**
- **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 485)**
- **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 489)**
- **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 491)**
- **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 490)**

- vlan *VLAN-ID* ip pim-dense ip-addr

```
Usage: ip pim-dense [ip-addr IP-ADDR|any]

Description: Set the source IP address for the PIM-DM packets sent out on this
             interface. You can either explicitly specify one of the existing
             VLAN's IP addresses or use 'any' option to dynamically determine
             it from the VLAN's current IP configuration. The default is 'any'.
             This command also enable the PIM-DM protocol on the VLAN interface.
```

Next Available Options:
- **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 476)**
- **any** -- Dynamically determine IP address.**(p. 466)**

- vlan *VLAN-ID* ip pim-dense ip-addr *IP-ADDR*

```
Specify IP address.
```

- vlan *VLAN-ID* ip pim-sparse ip-addr

```
Usage: ip pim-sparse [ip-addr IP-ADDR|any]

Description: Set the source IP address for the PIM-SM packets sent out on this
```

© 2007 Hewlett-Packard Development Company, L.P.

```
interface. You can either explicitly specify one of the existing
VLAN's IP addresses or use 'any' option to dynamically determine
it from the VLAN's current IP configuration. The default is 'any'.
This command also enable the PIM-SM protocol on the VLAN interface.
```

Next Available Options:

- **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 476)**
- **any** -- Dynamically determine IP address.**(p. 466)**

- vlan *VLAN-ID* ip pim-sparse ip-addr *IP-ADDR*

```
Specify IP address.
```

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* virtual-ip-address *IP-ADDR/MASK-LENGTH*

```
Specify IP address/mask.
```

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address *IP-ADDR*

```
Specify IP address.
```

ip-recv-mac-address

- [no] vlan *VLAN-ID* ip-recv-mac-address

```
Usage: [no] ip-recv-mac-address <macaddress> interval <1-255>

Description:  Associates a L3-mac-address with a VLAN.
      To associate L3-Mac-Address for a VLAN.
         ip-recv-mac-address <mac-address> interval <1-255>
      To associate L3-Mac-Address with a VLAN with default
      timeout interval of 60s.
         ip-recv-mac-address <mac-address>
      To disassociate L3-Mac_address with a VLAN.
            no ip-recv-mac-address
Parameters:
       <mac-address>  -  The L3-mac-address to be associated with a VLAN.
       interval       -  Specify L3-Mac-Address timeout interval.
       <1-255>        -  Timeout interval in seconds <1-255>.
```

Next Available Option:

- **mac-address** -- The L3-mac-address to be associated with a VLAN. (MAC-ADDR) **(p. 479)**

irdp

- [no] vlan *VLAN-ID* ip irdp

```
Usage: [no] ip irdp [...]

Description: Configure ICMP Router Discovery Protocol (IRDP). This is
             a VLAN context command. It can be called directly from the VLAN
             context or may follow the 'vlan VLAN-ID' command prefix.
             Called without parameters the command enables or disables (if
             preceded by 'no') the protocol on the VLAN specified, or
             identified by the current VLAN context. Use 'ip irdp ?' to get
             a list of all possible configurable parameters.
```

© 2007 Hewlett-Packard Development Company, L.P.

Next Available Options:

- **advert-address** < multicast | broadcast > -- Specify the destination address to be used for router advertisements**(p. 465)**
- **holdtime** < 4 to 9000 > -- Set the lifetime (in seconds) of the router advertisements sent on this interface**(p. 474)**
- **maxadvertinterval** < 4 to 1800 > -- Set the maximum time (in seconds) allowed between sending unsolicited router advertisements**(p. 480)**
- **minadvertinterval** < 3 to 1800 > -- Set the minimum time (in seconds) allowed between sending unsolicited router advertisements**(p. 481)**
- **preference** -- The preferability of the router as a default router, relative to the other routers on the same subnet**(p. 486)**

jumbo

- [no] vlan *VLAN-ID* jumbo

```
Usage: [no] jumbo

Description: Labels this VLAN as a Jumbo VLAN, allowing you to pass
             packets up to 9220 bytes in size.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

lan-prune-delay

- [no] vlan *VLAN-ID* ip pim-dense lan-prune-delay

```
Usage: [no] ip pim-dense lan-prune-delay

Description: Turn on/off the LAN Prune Delay Option on this interface.
             Default is 'on'.
```

- [no] vlan *VLAN-ID* ip pim-sparse lan-prune-delay

```
Usage: [no] ip pim-sparse lan-prune-delay

Description: Turn on/off the LAN Prune Delay Option on this interface.
             Default is 'on'.
```

lowest

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address lowest

```
Dynamically determine lowest IP address.
```

mac-address

- vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR*

```
The L3-mac-address to be associated with a VLAN.
```

Next Available Option:

- **interval** -- Specify the L3-Mac-Address timeout interval. **(p. 475)**

© 2007 Hewlett-Packard Development Company, L.P.

maxadvertinterval

- vlan *VLAN-ID* ip irdp maxadvertinterval *< 4 to 1800 >*

```
Usage: [no] ip irdp maxadvertinterval <4-1800>

Description: Set the maximum time (in seconds) allowed between sending
             unsolicited router advertisements.
```

Range: < 4 to 1800 >

max-graft-retries

- vlan *VLAN-ID* ip pim-dense max-graft-retries *< 1 to 10 >*

```
Usage: ip pim-dense max-graft-retries <1-10>

Description: Set the maximum number of times this router will resend a
             Graft on this interface. Default is 2.
```

Range: < 1 to 10 >

md5-auth-key-chain

- vlan *VLAN-ID* ip ospf md5-auth-key-chain

```
Set MD5 authentication method and key chain.
```

Next Available Option:

- **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 470)**

- vlan *VLAN-ID* ip ospf *IP-ADDR* md5-auth-key-chain

```
Set MD5 authentication method and key chain.
```

Next Available Option:

- **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 470)**

- vlan *VLAN-ID* ip ospf all md5-auth-key-chain

```
Set MD5 authentication method and key chain.
```

Next Available Option:

- **chain-name** -- Specify key chain to use for MD5 authentication. (ASCII-STR) **(p. 470)**

metric

- vlan *VLAN-ID* ip rip metric *< 1 to 15 >*

```
Set metric for this interface.
```

Range: < 1 to 15 >

- vlan *VLAN-ID* ip rip *IP-ADDR* metric *< 1 to 15 >*

```
Set metric for this interface.
```

Range: < 1 to 15 >

- vlan *VLAN-ID* ip rip all metric *< 1 to 15 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Set metric for this interface.
```

Range: < 1 to 15 >

minadvertinterval

- vlan *VLAN-ID* ip irdp minadvertinterval *< 3 to 1800 >*

```
Usage: [no] ip irdp minadvertinterval <3-1800>

Description: Set the minimum time (in seconds) allowed between sending
             unsolicited router advertisements. Must be no greater than the
             maximum time between sending unsolicited router advertisements.
```

Range: < 3 to 1800 >

mirror

- vlan *VLAN-ID* monitor all *< In | Out | Both >* mirror

```
Mirror destination.
```

Next Available Options:
- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 482)**
- **mirror_session_name** -- Mirror destination name.**(p. 481)**

- vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP < In >* mirror

```
Mirror destination.
```

Next Available Options:
- **monitor_mirror_session_id** < 1 to 4 > -- Mirror destination number.**(p. 482)**
- **mirror_session_name** -- Mirror destination name.**(p. 481)**

mirror_session_name

- [no] vlan *VLAN-ID* monitor all *< In | Out | Both >* mirror

```
Mirror destination name.
```

- [no] vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP < In >* mirror

```
Mirror destination name.
```

monitor

- [no] vlan *VLAN-ID* monitor

```
Usage: 1) [no] monitor all <in|out|both> mirror <1-4 | NAME-STR>
                [1-4 | NAME-STR]...
       2) [no] monitor ip access-group <ACL-NAME> <in> mirror
                <1-4 | NAME-STR> [1-4 | NAME-STR]...

Description: Define either the VLAN is to be monitored or not.
             The network traffic seen by the monitored VLAN is copied to
             the Mirroring Destination to which a network analyzer can be
             attached.
             Note: When mirroring a VLAN in a busy network,
             some frames may not be copied to the mirroring port.
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                This is an VLAN context command. It can be called directly
                from the VLAN context or follow the 'vlan VLAN-ID command.

Parameters:     o 1-4 - Mirror destination number
                o NAME-STR - Friendly name associated with the mirror
                destination number.
                o ACL-NAME - Standard or Extended Access Control List number.
                o <in|out|both> direction of the traffic to be monitored.
```

Next Available Options:

- **all** < In | Out | Both > -- Monitor all traffic.**(p. 465)**
- **ip** -- Apply an IPv4 access list.**(p. 476)**

monitor_mirror_ACL_dir

- vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >*

```
Usage: [no] mirror-port [[ethernet] PORT-NUM]

Description: Define the mirror port for diagnostic purposes. The device
             ports or VLAN (if VLANs are enabled on the device) that will
             be monitored are defined through the 'monitor' command in
             either VLAN or interface context.
             The network traffic seen by the monitored ports is copied to
             the mirror port to which a network analyzer can be attached.
             When mirroring multiple ports in a busy network,
             some frames may not be copied to the monitoring port.

Parameters:  PORT-NUM - Port that will be acting as the monitoring port. It
             cannot be a trunked port. The parameter must be specified,
             if the 'no' keyword is not used. Otherwise, it must not be
             present.
```

Supported Values:

- **In** -- Monitor inbound traffic permitted by the ACL

Next Available Option:

- **mirror** -- Mirror destination.**(p. 481)**

monitor_mirror_session_id

- [no] vlan *VLAN-ID* monitor all *< In | Out | Both >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

- [no] vlan *VLAN-ID* monitor ip access-group *ACCESS-GROUP* *< In >* mirror *< 1 to 4 >*

```
Mirror destination number.
```

Range: < 1 to 4 >

mroute

- vlan *VLAN-ID* ip mroute

```
Usage: ip mroute ...
```

© 2007 Hewlett-Packard Development Company, L.P.

```
Description: Configure IP Multicast Routing parameters on the VLAN
             interface. The command must be followed by a parameter.
             Use 'ip mroute ?' to get a list of all possible parameters.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Option:

- **ttl-threshold** < 0 to 255 > -- Set the multicast datagram TTL threshold for the interface**(p. 492)**

name

- vlan *VLAN-ID* name *NAME*

```
Usage: name ASCII-STR

Description: Set the VLAN's name.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

nbr-timeout

- vlan *VLAN-ID* ip pim-sparse nbr-timeout *< 60 to 8000 >*

```
Usage: ip pim-sparse nbr-timeout <60-8000>

Description: Set the neighbour loss time interval for this interface.
             Default is 180 seconds.
```

Range: < 60 to 8000 >

no-default

- vlan *VLAN-ID* ip irdp preference no-default

```
Indicates that the router should never be used as a default by its neighbors.
```

number

- vlan *VLAN-ID* ip irdp preference *< -2147483647 to 2147483647 >*

```
The router preferability number. Higher values are more preferable.
```

Range: < -2147483647 to 2147483647 >

ospf

- [no] vlan *VLAN-ID* ip ospf

```
Usage: [no] ip ospf [...]

Description: Enable/disable/configure Open Shortest Path First (OSPF)
             protocol on the VLAN interface.
             Called without 'no', the command enables OSPF on the interface.
             Otherwise ('no' is specified), the command disables OSPF on the
             interface. The command can be followed by an OSPF configuration
             command. Use 'ip ospf ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                from the VLAN context or follow the 'vlan VLAN-ID'
                command.
```

Next Available Options:

- **area** -- Specify an OSPF area.**(p. 466)**
- **authentication-key** -- Set simple authentication method and key.**(p. 467)**
- **authentication** -- Disable authentication.**(p. 467)**
- **md5-auth-key-chain** -- Set MD5 authentication method and key chain.**(p. 480)**
- **cost** < 1 to 65535 > -- Set metric of this interface.**(p. 470)**
- **dead-interval** < 1 to 65535 > -- Set dead interval in seconds; the default is 40.**(p. 471)**
- **hello-interval** < 1 to 65535 > -- Set hello interval in seconds; the default is 10.**(p. 473)**
- **priority** < 0 to 255 > -- Set priority of this router as a designated router.**(p. 487)**
- **retransmit-interval** < 1 to 3600 > -- Set retransmit interval in seconds; the default is 5.**(p. 490)**
- **transit-delay** < 1 to 3600 > -- Set transit delay in seconds; the default is 1.**(p. 492)**
- **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 476)**
- **all** -- Process the request for all IP addresses.**(p. 465)**

override-interval

- vlan *VLAN-ID* ip pim-dense override-interval *< 500 to 6000 >*

```
Usage: ip pim-dense override-interval <500-6000>

Description: Set the value inserted into the Override Interval field of
             a LAN Prune Delay option on this interface. Default is 2500
             milliseconds.
```

Range: < 500 to 6000 >

- vlan *VLAN-ID* ip pim-sparse override-interval *< 500 to 6000 >*

```
Usage: ip pim-sparse override-interval <500-6000>

Description: Set the value inserted into the Override Interval field of
             a LAN Prune Delay option on this interface. Default is 2500
             milliseconds.
```

Range: < 500 to 6000 >

owner

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* owner

```
Usage: vrrp vrid <VRID> owner

Description: Designate the virtual router instance as an Owner (Master).
             There is no default value.
```

pim-dense

- [no] vlan *VLAN-ID* ip pim-dense

```
Usage: [no] ip pim-dense [...]

Description: Enable/disable/configure PIM-DM protocol on the VLAN interface.
             Use direct and 'no' versions of the command to enable/disable
             PIM-DM on the interface. Use 'ip pim-dense ?' to get the list
             of all configuration options. This command can be used in the
```

© 2007 Hewlett-Packard Development Company, L.P.

```
VLAN context or in the global context with the 'vlan <VLAN-ID>'
prefix.
```

Next Available Options:

- **ip-addr** -- Set the source IP address for the PIM-DM packets sent out on this interface**(p. 476)**
- **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface**(p. 479)**
- **hello-interval** < 5 to 300 > -- Set the frequency at which PIM Hello messages are transmitted on this interface**(p. 473)**
- **hello-delay** < 0 to 5 > -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface**(p. 473)**
- **graft-retry-interval** < 1 to 10 > -- Set the interval a PIM router waits for a Graft Ack before resending a Graft on this interface**(p. 473)**
- **max-graft-retries** < 1 to 10 > -- Set the maximum number of times this router will resend a Graft on this interface**(p. 480)**
- **override-interval** < 500 to 6000 > -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface**(p. 484)**
- **propagation-delay** < 250 to 2000 > -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface**(p. 487)**
- **ttl-threshold** < 0 to 255 > -- Set the Time To Live in a PIM-DM State Refresh message at which it is not forwarded on this interface**(p. 492)**

pim-sparse

- [no] vlan *VLAN-ID* ip pim-sparse

```
Usage: [no] ip pim-sparse [...]

Description: Enable/disable/configure PIM-SM protocol on the VLAN interface.
             Use direct and 'no' versions of the command to enable/disable
             PIM-SM on the interface. Use 'ip pim-sparse ?' to get the list
             of all configuration options. This command can be used in the
             VLAN context or in the global context with the 'vlan <VLAN-ID>'
             prefix.
```

Next Available Options:

- **ip-addr** -- Set the source IP address for the PIM-SM packets sent out on this interface**(p. 476)**
- **lan-prune-delay** -- Turn on/off the LAN Prune Delay Option on this interface**(p. 479)**
- **hello-interval** < 5 to 300 > -- Set the frequency at which PIM Hello messages are transmitted on this interface**(p. 473)**
- **hello-delay** < 0 to 5 > -- Set the maximum time before a triggered PIM Hello message is transmitted on this interface**(p. 473)**
- **override-interval** < 500 to 6000 > -- Set the value inserted into the Override Interval field of a LAN Prune Delay option on this interface**(p. 484)**
- **propagation-delay** < 250 to 2000 > -- Set the value inserted into the LAN Prune Delay field of a LAN Prune Delay option on this interface**(p. 487)**
- **dr-priority** -- Set the priority value to use on the interface in the Designated Router election process**(p. 471)**
- **nbr-timeout** < 60 to 8000 > -- Set the neighbour loss time interval for this interface**(p. 483)**

poison-reverse

- [no] vlan *VLAN-ID* ip rip poison-reverse

```
Enable/disable poison reverse on this interface.
```

© 2007 Hewlett-Packard Development Company, L.P.

- [no] vlan *VLAN-ID* ip rip *IP-ADDR* poison-reverse

  ```
  Enable/disable poison reverse on this interface.
  ```

- [no] vlan *VLAN-ID* ip rip all poison-reverse

  ```
  Enable/disable poison reverse on this interface.
  ```

port-name

- [no] vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR* *< dns | ntp | netbios-ns | ... >*

  Supported Values:
  - **dns** -- Domain Name Service (53)
  - **ntp** -- Network Time Protocol (123)
  - **netbios-ns** -- NetBIOS Name Service (137)
  - **netbios-dgm** -- NetBIOS Datagram Service (138)
  - **radius** -- Remote Authentication Dial-In User Service (1812)
  - **radius-old** -- Remote Authentication Dial-In User Service (1645)
  - **rip** -- Routing Information Protocol (520)
  - **snmp** -- Simple Network Management Protocol (161)
  - **snmp-trap** -- Simple Network Management Protocol (162)
  - **tftp** -- Trivial File Transfer Protocol (69)
  - **timep** -- Time Protocol (37)

port-num

- [no] vlan *VLAN-ID* ip forward-protocol udp *IP-ADDR TCP/UDP-PORT*

  ```
  UDP port number of the server.
  ```

preempt-mode

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* preempt-mode

  ```
  Usage: [no] vrrp vrid <VRID> preempt-mode

  Description: Enable/disable preempt mode for the virtual router instance.
               The default value is 'enabled'.
  ```

preference

- vlan *VLAN-ID* ip irdp preference

  ```
  Usage: [no] ip irdp preference <no-default|<-2147483647-2147483647>>

  Description: The preferability of the router as a default
               router, relative to the other routers on the same
               subnet.  Higher values are more preferable.
  ```

  Next Available Options:
  - **number** < -2147483647 to 2147483647 > -- The router preferability number. Higher values are more preferable.**(p. 483)**
  - **no-default** -- Indicates that the router should never be used as a default by its neighbors.**(p. 483)**

© 2007 Hewlett-Packard Development Company, L.P.

primary-ip-address

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* primary-ip-address

```
Usage: [no] vrrp vrid <VRID> primary-ip-address <IP-ADDR | lowest>

Description: Specify IP address the virtual router instance will use as
             a source in VRRP advertisement messages. If not set (i.e. is
             '0.0.0.0') the virtual router uses numerically lowest IP address
             of the VLAN. The default value is 'lowest'.
```

Next Available Options:

- **ip-addr** -- Specify IP address. (IP-ADDR) **(p. 476)**
- **lowest** -- Dynamically determine lowest IP address.**(p. 479)**

priority

- vlan *VLAN-ID* ip ospf priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- vlan *VLAN-ID* ip ospf all priority *< 0 to 255 >*

```
Set priority of this router as a designated router.
```

Range: < 0 to 255 >

- vlan *VLAN-ID* qos priority *< 0 | 1 | 2 | ... >*

```
Specify priority to use.
```

Supported Values:

- **0**
- **1**
- **2**
- **3**
- **4**
- **5**
- **6**
- **7**

- vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* priority *< 1 to 255 >*

```
Usage: vrrp vrid <VRID> priority <1-255>

Description: Configure priority for the virtual router instance.
             The default value is '100'.
```

Range: < 1 to 255 >

propagation-delay

- vlan *VLAN-ID* ip pim-dense propagation-delay *< 250 to 2000 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: ip pim-dense propagation-delay <250-2000>

Description: Set the value inserted into the LAN Prune Delay field of a
             LAN Prune Delay option on this interface. Default is 500
             milliseconds.
```

Range: < 250 to 2000 >

- vlan *VLAN-ID* ip pim-sparse propagation-delay *< 250 to 2000 >*

```
Usage: ip pim-sparse propagation-delay <250-2000>

Description: Set the value inserted into the LAN Prune Delay field of a
             LAN Prune Delay option on this interface. Default is 500
             milliseconds.
```

Range: < 250 to 2000 >

protocol

- vlan *VLAN-ID* protocol

```
Set a predefined protocol for the current VLAN.
```

Next Available Options:

- **protocols** < IPX | IPv4 | IPv6 | ... > -- Set a predefined protocol for the current VLAN. **(p. 488)**
- **protocol-group** -- Enter a list of protocols for the current VLAN delimited by commas. (ASCII-STR) **(p. 488)**

protocol-group

- [no] vlan *VLAN-ID* protocol *PROTOCOL-GROUP*

```
Enter a list of protocols for the current VLAN delimited by commas.
```

protocols

- [no] vlan *VLAN-ID* protocol *< IPX | IPv4 | IPv6 | ... >*

```
Set a predefined protocol for the current VLAN.
```

Supported Values:

- **IPX** -- IPX Protocol Group
- **IPv4** -- IP version 4 Protocol Group
- **IPv6** -- IP version 6 Protocol Group
- **ARP** -- Address Resolution Protocol Group
- **Appletalk** -- Appletalk Protocol Group
- **SNA** -- System Network Architecture Protocol Group
- **NetBEUI** -- Network BIOS Enhanced User Interface Protocol Group

proxy-arp

- [no] vlan *VLAN-ID* ip proxy-arp

```
Usage: [no] ip proxy-arp

Description: Enable/disable proxy ARP. This is a VLAN context command.
             It can be called directly from the VLAN context or may follow
             the 'vlan VLAN-ID' command prefix. When proxy ARP is enabled on
             a VLAN, the device responds to ARP requests received on the
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                VLAN ports when the device knows a route to the requested IP
                addresses.
```

qos

- [no] vlan *VLAN-ID* qos

```
Usage: [no] qos [dscp <000000|000001...111111> | priority <0-7>]

Description: Set VLAN-based priority. The 'dscp' or 'priority' must
             be specified if 'no' is not used. Using 'no' configures
             the switch not to apply a VLAN priority override to this
             VLAN's packets.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:

- **dscp** < 000000 | 000001 | 000010 | ... > -- Specify DSCP policy to use. **(p. 471)**
- **priority** < 0 | 1 | 2 | ... > -- Specify priority to use. **(p. 487)**

querier

- [no] vlan *VLAN-ID* ip igmp querier

```
Usage: [no] ip igmp querier

Description: Specify querier/non-querier capability for the VLAN. IGMP
             queries are not sent when the mode is disabled. When
             enabled, the device cannot become Querier for the subnet
             unless the VLAN has an IP Address (use the 'show ip' command
             to determine this).  Each subnet must have at least one IGMP
             Querier-capable device in order for IGMP to function
             properly.
```

receive

- vlan *VLAN-ID* ip rip receive *< V1-only | V2-only | V1-or-V2 | ... >*

```
Define RIP version for incoming packets.
```

Supported Values:

- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

- vlan *VLAN-ID* ip rip *IP-ADDR* receive *< V1-only | V2-only | V1-or-V2 | ... >*

```
Define RIP version for incoming packets.
```

Supported Values:

- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

- vlan *VLAN-ID* ip rip all receive *< V1-only | V2-only | V1-or-V2 | ... >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Define RIP version for incoming packets.
```

Supported Values:
- **V1-only** -- Accept RIP version 1 updates only.
- **V2-only** -- Accept RIP version 2 updates only.
- **V1-or-V2** -- Accept both RIP 1 and RIP 2 updates.
- **disabled** -- Do not accept RIP updates.

retransmit-interval

- vlan *VLAN-ID* ip ospf retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

- vlan *VLAN-ID* ip ospf all retransmit-interval *< 1 to 3600 >*

```
Set retransmit interval in seconds; the default is 5.
```

Range: < 1 to 3600 >

rip

- [no] vlan *VLAN-ID* ip rip

```
Usage: [no] ip rip [...]

Description: Enable/disable/configure Routing Internet Protocol (RIP)
             on the VLAN interface.
             Called without 'no', the command enables RIP on the interface.
             Otherwise ('no' is specified), the command disables RIP on the
             interface. The command can be followed by a RIP configuration
             command. Use 'ip rip ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Options:
- **authentication-type** < none | text > -- Set authentication type used on this interface.**(p. 468)**
- **authentication-key** -- Set authentication key.**(p. 467)**
- **metric** < 1 to 15 > -- Set metric for this interface.**(p. 480)**
- **poison-reverse** -- Enable/disable poison reverse on this interface.**(p. 485)**
- **receive** < V1-only | V2-only | V1-or-V2 | ... > -- Define RIP version for incoming packets.**(p. 489)**
- **send** < disabled | V1-only | V1-compatible-V2 | ... > -- Define RIP version for outgoing packets.**(p. 491)**
- **rip-compatible** < V1-only | V2-only | V1-or-V2 > -- Define RIP version for incoming and outgoing packets.**(p. 490)**
- **ip-addr** -- Specify the IP address the request is for. (IP-ADDR) **(p. 476)**
- **all** -- Process the request for all IP addresses.**(p. 465)**

rip-compatible

- vlan *VLAN-ID* ip rip *< V1-only | V2-only | V1-or-V2 >*

© 2007 Hewlett-Packard Development Company, L.P.

```
Define RIP version for incoming and outgoing packets.
```

Supported Values:
- **V1-only** -- Use RIP version 1 only.
- **V2-only** -- Use RIP version 2 only.
- **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.

■ vlan *VLAN-ID* ip rip *IP-ADDR* *< V1-only | V2-only | V1-or-V2 >*

```
Define RIP version for incoming and outgoing packets.
```

Supported Values:
- **V1-only** -- Use RIP version 1 only.
- **V2-only** -- Use RIP version 2 only.
- **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.

■ vlan *VLAN-ID* ip rip all *< V1-only | V2-only | V1-or-V2 >*

```
Define RIP version for incoming and outgoing packets.
```

Supported Values:
- **V1-only** -- Use RIP version 1 only.
- **V2-only** -- Use RIP version 2 only.
- **V1-or-V2** -- Use RIP 2 in the RIP 1 compatible mode.

send

■ vlan *VLAN-ID* ip rip send *< disabled | V1-only | V1-compatible-V2 | ... >*

```
Define RIP version for outgoing packets.
```

Supported Values:
- **disabled** -- Do not send RIP updates.
- **V1-only** -- Send RIP version 1 updates only.
- **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
- **V2-only** -- Send RIP version 2 updates only.

■ vlan *VLAN-ID* ip rip *IP-ADDR* send *< disabled | V1-only | V1-compatible-V2 | ... >*

```
Define RIP version for outgoing packets.
```

Supported Values:
- **disabled** -- Do not send RIP updates.
- **V1-only** -- Send RIP version 1 updates only.
- **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
- **V2-only** -- Send RIP version 2 updates only.

■ vlan *VLAN-ID* ip rip all send *< disabled | V1-only | V1-compatible-V2 | ... >*

```
Define RIP version for outgoing packets.
```

Supported Values:
- **disabled** -- Do not send RIP updates.
- **V1-only** -- Send RIP version 1 updates only.
- **V1-compatible-V2** -- Send RIP 2 updates using RFC 1058 route subsumption.
- **V2-only** -- Send RIP version 2 updates only.

src-ip

■ vlan *VLAN-ID* connection-rate-filter unblock *IP-ADDR/MASK-LENGTH*

```
Match packets from the specified subnet.
```

© 2007 Hewlett-Packard Development Company, L.P.

tagged

- [no] vlan *VLAN-ID* tagged *[ETHERNET] PORT-LIST*

```
Usage: [no] tagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as tagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

timer-interval

- vlan *VLAN-ID* ip-recv-mac-address *MAC-ADDR* interval *< 1 to 255 >*

```
Timeout interval in seconds <1-255>.
```

Range: < 1 to 255 >

transit-delay

- vlan *VLAN-ID* ip ospf transit-delay *< 1 to 3600 >*

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

- vlan *VLAN-ID* ip ospf *IP-ADDR* transit-delay *< 1 to 3600 >*

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

- vlan *VLAN-ID* ip ospf all transit-delay *< 1 to 3600 >*

```
Set transit delay in seconds; the default is 1.
```

Range: < 1 to 3600 >

ttl-threshold

- vlan *VLAN-ID* ip pim-dense ttl-threshold *< 0 to 255 >*

```
Usage: ip pim-dense ttl-threshold <0-255>

Description: Set the Time To Live in a PIM-DM State Refresh message at
             which it is not forwarded on this interface. Default is 0.
```

Range: < 0 to 255 >

- vlan *VLAN-ID* ip mroute ttl-threshold *< 0 to 255 >*

```
Usage: ip mroute ttl-threshold <0-255>

Description: Set the multicast datagram TTL threshold for the interface.
             Any IP multicast datagrams with a TTL less than this threshold
             will not be forwarded out the interface. The default value of 0
             means all multicast packets are forwarded out the interface.
```

Range: < 0 to 255 >

udp

- [no] vlan *VLAN-ID* ip forward-protocol udp

© 2007 Hewlett-Packard Development Company, L.P.

```
Usage: [no] ip forward-protocol udp IP-ADDR PORT-NUM|PORT-NAME

Description: Add or remove a UDP server address for the VLAN. The
             broadcast  packets received by the switch on this VLAN are to
             be forwarded to the specified application server.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

Next Available Option:

- **ip-addr** -- IP address of the protocol server. (IP-ADDR) **(p. 476)**

unblock

- vlan *VLAN-ID* connection-rate-filter unblock

```
Resets a host previously blocked by the connection rate filter
```

Next Available Options:

- **all** -- Resets all previously blocked by the connection rate filter **(p. 465)**
- **host** -- Match packets from the specified IP address. (IP-ADDR) **(p. 474)**
- **src-ip** -- Match packets from the specified subnet. (IP-ADDR/MASK-LENGTH) **(p. 491)**

untagged

- [no] vlan *VLAN-ID* untagged *[ETHERNET] PORT-LIST*

```
Usage: [no] untagged [ethernet] PORT-LIST

Description: Assign ports to current VLAN as untagged.
             This is a VLAN context command. It can be called directly
             from the VLAN context or follow the 'vlan VLAN-ID'
             command.
```

virtual-ip-address

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >* virtual-ip-address

```
Usage: [no] vrrp vrid <VRID> virtual-ip-address <IP-ADDR>

Description: Specify IP address to be supported by the virtual router instance.
             There is no default value.
```

Next Available Option:

- **ip-addr** -- Specify IP address/mask. (IP-ADDR/MASK-LENGTH) **(p. 476)**

voice

- [no] vlan *VLAN-ID* voice

```
Usage: [no] voice

Description: Labels this VLAN as a Voice VLAN, allowing you to separate,
             prioritize, and authenticate voice traffic moving through
             your network.
             This is a VLAN context command. It can be called directly
```

© 2007 Hewlett-Packard Development Company, L.P.

```
                from the VLAN context or follow the 'vlan VLAN-ID'
                command.
```

vrid

- [no] vlan *VLAN-ID* vrrp vrid *< 1 to 255 >*

```
Usage: [no] vrrp vrid <VRID> [...]

Description: Configure a virtual router instance for the VLAN.
             A virtual router is defined by its virtual router
             identifier (VRID) and a set of IP addresses for which
             virtual router acts as a Master or Backup. The scope
             of each virtual router is restricted to a single VLAN.
```

Range: < 1 to 255 >

Next Available Options:

- **backup** -- Designate the virtual router instance as a Backup**(p. 469)**
- **owner** -- Designate the virtual router instance as an Owner (Master)**(p. 484)**
- **virtual-ip-address** -- Specify IP address to be supported by the virtual router instance**(p. 493)**
- **primary-ip-address** -- Specify IP address the virtual router instance will use as a source in VRRP advertisement messages**(p. 487)**
- **advertise-interval** < 1 to 255 > -- Set time interval (in seconds) between sending VRRP advertisement messages**(p. 465)**
- **priority** < 1 to 255 > -- Configure priority for the virtual router instance**(p. 487)**
- **preempt-mode** -- Enable/disable preempt mode for the virtual router instance**(p. 486)**
- **enable** -- Enable/disable operation of the virtual router instance**(p. 472)**

vrrp

- [no] vlan *VLAN-ID* vrrp

```
Usage: [no] vlan <VLAN-ID> vrrp vrid <VRID> [...]

Description: Enable/disable/configure VRRP operation on the VLAN.
             Use 'vrrp vrid <VRID> ?' to get a list of all possible options.
             This is a VLAN context command. It can be called directly from
             the VLAN context or follow the 'vlan VLAN-ID' command.
```

Next Available Option:

- **vrid** < 1 to 255 > -- Configure a virtual router instance for the VLAN**(p. 494)**

© 2007 Hewlett-Packard Development Company, L.P.

walkMIB

OVERVIEW

Category:	SNMP
Primary context:	manager
Related Commands	setMIB (page 314)

```
Usage: walkmib OBJECT-STR [OBJECT-STR ...]

Description: Walk through all instances of the object specified displaying
             the MIB object names, instances and values.
```

COMMAND STRUCTURE

- walkMIB **object** -- The mib object to start from. (ASCII-STR) **(p. 495)**

EXAMPLES

Example: walkMIB

Walk the MIB objects in CdpCacheEntry:

```
HPswitch # walkmib CdpCacheEntry
cdpCacheAddressType.1.2 = 1
cdpCacheAddressType.3.1 = 1
cdpCacheAddress.1.2 = 42 3c  a4 0b
cdpCacheAddress.3.1 = 7f 00  00 01
cdpCacheVersion.1.2 = Revision F.02.C1 /sw/code/build/info(f00)
cdpCacheVersion.3.1 = Revision C.09.02 /sw/code/build/vgro(c09)
cdpCacheDeviceId.1.2 = HP ProCurve Switch 2512(005004-18df9c)
cdpCacheDeviceId.3.1 = HP4000(0060b0-fc904b)
cdpCacheDevicePort.1.2 = 12
cdpCacheDevicePort.3.1 = A4
cdpCachePlatform.1.2 = HP J4812A ProCurve Switch 2512
cdpCachePlatform.3.1 = HP J4121A ProCurve Switch 4000M
cdpCacheCapabilities.1.2 = 8
cdpCacheCapabilities.3.1 = 8
```

COMMAND DETAILS

object (p. 495)

object

- walkMIB *OBJECT*

  The mib object to start from.

© 2007 Hewlett-Packard Development Company, L.P.

web-management

OVERVIEW

Category:	Switch Management
Primary context:	config
Related Commands	**show config (page 341)** **crypto (page 107)** **crypto (page 107)**

```
Usage: [no] web-management [management-url] URL
                           [support-url] URL
                           [<plaintext | ssl [<TCP-PORT>] >]

Description: Enable/disable the device web server.

Parameters:

    o management-url - Specify URL to load when the [?] button is clicked
             on the device's web interface.

    o support-url - Specify URL to load when the Support tab is clicked
             on the device's web interface.

    o plaintext - optional keyword indicating that the http server should
             be enabled with no security.  If no parameters are specified,
             'plaintext' is implied.

    o ssl - required keyword indicating that the http server should be
             enabled with Secure Sockets Layer support.
             Note: The 'ssl' and 'plaintext' variants of the command
             function independently of each other.  Enabling http+ssl does
             not automatically prevent the device from accepting plaintext
             connections; you must explicitly disable plaintext connections
             with the command 'no web-management plaintext'

    o TCP-PORT - optional - TCP port on which the https server should listen
             for connections.  If not specified, this defaults to port 443.
             This is configurable for ssl connections only; the plaintext
             server always listens on the well-known port 80.
```

COMMAND STRUCTURE

- [no] web-management **management-url** -- Specify URL for web interface [?] button. **(p. 497)**
  - **management-url** -- Specify URL for web interface [?] button. (ASCII-STR) **(p. 497)**
- [no] web-management **plaintext** -- Enable/disable the http server (insecure). **(p. 497)**
- [no] web-management **ssl** -- Enable/disable the https server (secure). **(p. 497)**
  - **ssl-port** -- TCP port on which https server should accept connections. (TCP/UDP-PORT) **(p. 497)**
- [no] web-management **support-url** -- Specify URL for web interface Support page. **(p. 497)**
  - **support-url** -- Specify URL for web interface Support page. (ASCII-STR) **(p. 497)**

© 2007 Hewlett-Packard Development Company, L.P.

EXAMPLES

Example: web-management

Re-enable insecure web browser access:

```
ProCurve(config)# web-management
```

COMMAND DETAILS

management-url (p. 497)	**ssl (p. 497)**	**support-url (p. 497)**
plaintext (p. 497)	**ssl-port (p. 497)**	

management-url

- [no] web-management management-url

```
Specify URL for web interface [?] button.
```

Next Available Option:

- **management-url** -- Specify URL for web interface [?] button. (ASCII-STR) **(p. 497)**

- web-management management-url *MANAGEMENT-URL*

```
Specify URL for web interface [?] button.
```

plaintext

- [no] web-management plaintext

```
Enable/disable the http server (insecure).
```

ssl

- [no] web-management ssl

```
Enable/disable the https server (secure).
```

Next Available Option:

- **ssl-port** -- TCP port on which https server should accept connections. (TCP/UDP-PORT) **(p. 497)**

ssl-port

- web-management ssl *TCP/UDP-PORT*

```
TCP port on which https server should accept connections.
```

support-url

- [no] web-management support-url

```
Specify URL for web interface Support page.
```

Next Available Option:

- **support-url** -- Specify URL for web interface Support page. (ASCII-STR) **(p. 497)**

© 2007 Hewlett-Packard Development Company, L.P.

- web-management support-url *SUPPORT-URL*

  Specify URL for web interface Support page.

© 2007 Hewlett-Packard Development Company, L.P.

write

OVERVIEW

Category:	Switch Management
Primary context:	manager
Related Commands	**show config (page 341)**

```
Usage: write <memory|terminal>

Description: View or save the running configuration of the switch.

             write terminal - displays the running configuration of the
                              switch on the terminal
             write memory   - saves the running configuration of the
                              switch to flash. The saved configuration
                              becomes the boot-up configuration of the switch
                              the next time it is booted.
```

COMMAND STRUCTURE

- write **memory** -- Save the running configuration of the switch to flash. **(p. 499)**
- write **terminal** -- Display the running configuration of the switch on the terminal. **(p. 499)**

EXAMPLES

Example: write memory

Make a configuration change (in this example, create a static IP route) and save the change to the configuration file in flash memory:

```
ProCurve(config)# ip route 192.0.0.0 255.0.0.0 195.1.1.1
ProCurve(config)# write memory
```

COMMAND DETAILS

memory (p. 499)	**terminal (p. 499)**

memory

- write memory

```
Save the running configuration of the switch to flash.
```

terminal

- write terminal

```
Display the running configuration of the switch on the terminal.
```

© 2007 Hewlett-Packard Development Company, L.P.

Technical information in this document is subject to change without notice.

© Copyright 2007 Hewlett-Packard Development Company, L.P. All rights reserved. Reproduction, adaptation, or translation without prior written permission is prohibited except as allowed under the copyright laws.

February 2007

Manual Part Number
5991-6257