The products, specifications, and other technical information regarding the products contained in this document are subject to change without notice. All information in this document is believed to be accurate and reliable, but is presented without warranty of any kind, express or implied, and users must take full responsibility for their application of any products specified in this document. Avaya disclaims responsibility for errors which may appear in this document, and it reserves the right, in its sole discretion and without notice, to make substitutions and modifications in the products and practices described in this document.

Microsoft, Windows, Windows NT, Windows 95, Windows 98, and Internet Explorer are trademarks or registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and other countries.

Sybase is a registered trademark of Sybase, Inc.

Novell, NDS, Netware, and Novell Directory Services are registered trademarks of Novell, Inc.

Solaris is a trademark of Sun Microsystems, Inc.

Intel and Pentium are registered trademarks of Intel Corporation.

ALL OTHER TRADEMARKS MENTIONED IN THIS DOCUMENT ARE PROPERTY OF THEIR RESPECTIVE OWNERS.
# Table of Contents

## Chapter 1 — Overview

Command Mode Summaries .................................................. 1-1  
Entering and Exiting the Command Modes ................................ 1-2  
Basic Functions .................................................................. 1-3  
Accessing the CLI .............................................................. 1-5

## Chapter 2 — AFT

Overview ................................................................. 2-1  
`clear aft instance invalid-learned-entries vlan` ...................... 2-2  
`clear aft instance learned-entries vlan` ............................. 2-3  
set aft agetime ............................................................ 2-4  
set aft auto-sizing-threshold ............................................ 2-5  
set aft entry ................................................................ 2-6  
set aft instance vlan (auto-increment) ................................. 2-10  
set aft instance vlan (hash-table-size) ............................... 2-11  
set aft super-agetime ..................................................... 2-12  
show aft config ............................................................. 2-13  
show aft entry ............................................................... 2-14  
show aft instance .......................................................... 2-16

## Chapter 3 — Appletalk

Overview ................................................................. 3-1  
appletalk access-group .................................................... 3-2  
appletalk access-list ...................................................... 3-3  
appletalk address .......................................................... 3-5  
appletalk admin-state ..................................................... 3-6  
appletalk cable-range ..................................................... 3-7  
appletalk echo .............................................................. 3-8  
appletalk mac-format ..................................................... 3-9  
appletalk routing ........................................................... 3-10  
appletalk static cable-range .............................................. 3-11  
appletalk vlan .............................................................. 3-13  
appletalk zone .............................................................. 3-14  
clear appletalk arp ......................................................... 3-15  
clear appletalk route ....................................................... 3-16  
clear appletalk traffic ..................................................... 3-17  
ping appletalk .............................................................. 3-18  
show appletalk access-list .............................................. 3-19  
show appletalk arp ........................................................ 3-20
# Table of Contents

- **Chapter 4 — Buffering**
  - Overview ........................................... 4-1
  - set buffering fabric-port (age-timer) .................. 4-2
  - set buffering fabric-port (hipri-alloc) ................. 4-3
  - set buffering fabric-port (hipri-service-ratio) ........ 4-4
  - set buffering fabric-port (pri-threshold) ............... 4-5
  - set buffering port (age-timer) ........................ 4-6
  - set buffering port (hipri-alloc) ....................... 4-7
  - set buffering port (hipri-service-ratio) ............... 4-8
  - set buffering port (pri-threshold) ..................... 4-9
  - show buffering fabric-port ............................. 4-10
  - show buffering port .................................. 4-11

- **Chapter 5 — Console** ................................ 5-1
  - Overview ........................................... 5-1
  - set console baud ..................................... 5-2
  - set console databits .................................. 5-3
  - set console flowcontrol .............................. 5-4
  - set console initcmd .................................. 5-5
  - set console parity ................................... 5-6
  - set console stopbits ................................. 5-7
  - set console transfer ppp .............................. 5-8
  - set console type .................................... 5-9
  - show console ........................................ 5-10

- **Chapter 6 — DNS** ..................................... 6-1
  - Overview ........................................... 6-1
  - ip domain-lookup .................................... 6-2
  - ip name-server ...................................... 6-3
  - ip domain-list ...................................... 6-4
  - ip domain-name ..................................... 6-5
  - show host .......................................... 6-6

- **Chapter 7 — DVMRP** ................................... 7-1
  - Overview ........................................... 7-1
  - ip dvmrp ............................................ 7-2
  - ip dvmrp interface-metric ............................. 7-3
  - ip dvmrp interface type ............................... 7-4
<table>
<thead>
<tr>
<th>ip dvmrp min-route-flash-update</th>
<th>7-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dvmrp neighbor-probe-interval</td>
<td>7-6</td>
</tr>
<tr>
<td>ip dvmrp neighbor-timeout</td>
<td>7-7</td>
</tr>
<tr>
<td>ip dvmrp prune-message-lifetime.</td>
<td>7-8</td>
</tr>
<tr>
<td>ip dvmrp remote-tunnel-address.</td>
<td>7-9</td>
</tr>
<tr>
<td>ip dvmrp route-limit</td>
<td>7-10</td>
</tr>
<tr>
<td>ip dvmrp stats-reset</td>
<td>7-11</td>
</tr>
<tr>
<td>ip dvmrp timers basic</td>
<td>7-12</td>
</tr>
<tr>
<td>ip multicast prune-source</td>
<td>7-13</td>
</tr>
<tr>
<td>ip multicast ttl-threshold.</td>
<td>7-14</td>
</tr>
<tr>
<td>router dvmrp</td>
<td>7-15</td>
</tr>
<tr>
<td>show ip dvmrp</td>
<td>7-16</td>
</tr>
<tr>
<td>show ip dvmrp designated forwarders</td>
<td>7-17</td>
</tr>
<tr>
<td>show ip dvmrp downstream dependent routers</td>
<td>7-18</td>
</tr>
<tr>
<td>show ip dvmrp forwarding cache</td>
<td>7-19</td>
</tr>
<tr>
<td>show ip dvmrp interface</td>
<td>7-20</td>
</tr>
<tr>
<td>show ip dvmrp interface neighbors</td>
<td>7-21</td>
</tr>
<tr>
<td>show ip dvmrp routes</td>
<td>7-22</td>
</tr>
</tbody>
</table>

**Chapter 8 — Hunt Groups** ........................................ 8-1

Overview ......................................................... 8-1
set huntgroup ................................................. 8-2
set huntgroup auto-flush ....................................... 8-3
set huntgroup (redistribute) ................................. 8-4
set huntgroup internal-error-shutdown ....................... 8-5
show huntgroup .................................................. 8-6
show huntgroup detailed ........................................ 8-7
show huntgroup internal-error-config ....................... 8-8

**Chapter 9 — IGMP** ............................................. 9-1

Overview ......................................................... 9-1
ip igmp .......................................................... 9-2
ip igmp max-groups ............................................... 9-3
ip igmp process-leaves .......................................... 9-4
ip igmp querier .................................................. 9-5
ip igmp querier-timeout ......................................... 9-6
ip igmp query-interval .......................................... 9-7
ip igmp query-max-response-time ............................... 9-8
ip igmp query-timeout ........................................... 9-9
ip igmp robustness ............................................... 9-10
ip igmp version .................................................. 9-11
ip mtrace .......................................................... 9-12
mtrace ............................................................... 9-13
router igmp ........................................................ 9-14
show ip igmp groups ............................................... 9-15
show ip igmp interface ........................................... 9-16
show ip igmp statistics ......................................... 9-17
## Table of Contents

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip route</td>
<td>11-59</td>
</tr>
<tr>
<td>show ip route summary</td>
<td>11-60</td>
</tr>
<tr>
<td>show ip short-lived</td>
<td>11-61</td>
</tr>
<tr>
<td>show ip traffic</td>
<td>11-62</td>
</tr>
<tr>
<td>show tcp configuration</td>
<td>11-63</td>
</tr>
<tr>
<td>show tcp connections</td>
<td>11-64</td>
</tr>
<tr>
<td>show tcp statistics</td>
<td>11-65</td>
</tr>
<tr>
<td>show udp statistics</td>
<td>11-66</td>
</tr>
</tbody>
</table>

### Chapter 12 — IP-RIP — 12-1

- Overview: 12-1
- default-metric: 12-2
- ip rip authentication key: 12-3
- ip rip authentication mode: 12-4
- ip rip default-route-mode: 12-5
- ip rip poison-reverse: 12-6
- ip rip receive version: 12-7
- ip rip send version: 12-8
- ip rip send-receive-mode: 12-9
- network: 12-10
- output-delay: 12-11
- router rip: 12-12
- timers basic: 12-13
- triggered updates: 12-14
- show ip rip statistics: 12-15

### Chapter 13 — IPX — 13-1

- Overview: 13-1
- clear ipx route: 13-3
- clear ipx service: 13-4
- ipx advertise-default-route-only: 13-5
- ipx default-route: 13-6
- ipx delay: 13-7
- ipx down: 13-8
- ipx gns-reply-disable: 13-9
- ipx gns-response-delay: 13-10
- ipx network: 13-11
- ipx output-rip-delay: 13-13
- ipx output-sap-delay: 13-14
- ipx rip: 13-15
- ipx rip-filter: 13-16
- ipx rip-max-packetsize: 13-18
- ipx rip-multiplier: 13-19
- ipx route: 13-20
- ipx router: 13-21
- ipx routing: 13-22
- ipx sap: 13-23
- ipx sap-max-packetsize: 13-24
Table of Contents

ipx sap-multiplier .............................................. 13-25
ipx sap-name-filter ........................................... 13-26
ipx sap-network-filter ....................................... 13-28
ipx send-receive-mode ....................................... 13-30
ipx send-triggered-updates ................................. 13-31
ipx service ....................................................... 13-32
ipx type-20-propagation ...................................... 13-34
ipx update interval ........................................... 13-35
ipx vlan ........................................................... 13-36
show ipx cache .................................................. 13-37
show ipx interface ............................................. 13-38
show ipx rip statistics ........................................ 13-39
show ipx rip-filter ............................................ 13-40
show ipx route .................................................. 13-41
show ipx sap statistics ....................................... 13-42
show ipx sap-name-filter ...................................... 13-43
show ipx sap-network-filter .................................. 13-44
show ipx service ................................................ 13-45
show ipx traffic ................................................ 13-46

Chapter 14 — Layer 3 Forwarding Cache ......................... 14-1

Overview ......................................................... 14-1
ip multicast route-cache aging ............................... 14-2
ip multicast route-cache hash-mode ......................... 14-3
ip multicast route-cache max-size .......................... 14-4
ip multicast route-cache readd-timeout .................... 14-5
ip multicast route-cache update-timeout ................... 14-7
ip unicast route-cache aging ................................ 14-8
ip unicast route-cache hash-mode ............................ 14-9
ip unicast route-cache max-size ............................. 14-10
ip unicast route-cache update-timeout ..................... 14-11
ipx route-cache aging ......................................... 14-12
ipx route-cache hash-mode .................................... 14-13
ipx route-cache max-size ...................................... 14-14
ipx route-cache update-timeout .............................. 14-15
show ip multicast cache ....................................... 14-16
show ip unicast cache .......................................... 14-17
show ipx cache .................................................. 14-18

Chapter 15 — LDAP ............................................. 15-1

Overview ......................................................... 15-1
ldap execution-option ......................................... 15-2
ldap search-base ............................................... 15-3
ldap server primary .......................................... 15-4
ldap server secondary ......................................... 15-5
show ldap ......................................................... 15-6
# Chapter 16 — Logging

Overview ................................................................. 16-1
logging clear ......................................................... 16-2
logging console ..................................................... 16-3
logging history ...................................................... 16-6
logging history size ............................................... 16-9
logging protocol event ........................................... 16-10
logging shutdown size ............................................ 16-12
logging traps ....................................................... 16-13
set syslog ............................................................ 16-15
set syslog facility .................................................. 16-16
set syslog server_ip ............................................... 16-19
set syslog severity ............................................... 16-20
show alarms ........................................................ 16-21
show logging ........................................................ 16-22
show syslog buffer ................................................ 16-23
show syslog config ............................................... 16-24

# Chapter 17 — Module

Overview ............................................................... 17-1
reset-module ......................................................... 17-2
set module name ................................................... 17-3
set module notes ................................................... 17-4
show module ....................................................... 17-5
show module inventory ........................................... 17-6

# Chapter 18 — NEDR and IEDR

Overview .............................................................. 18-1
set huntgroup internal-error-shutdown ....................... 18-2
set internal-error-threshold ..................................... 18-3
set port internal-error-shutdown ............................... 18-4
set port network-error-detection ............................... 18-5
show huntgroup internal-error-config ......................... 18-7
show port internal-error-config ............................... 18-8
show port network-error detection ............................ 18-9

# Chapter 19 — OSPF

Overview .............................................................. 19-1
area ................................................................. 19-3
area ase-filter ...................................................... 19-4
area default-cost .................................................. 19-5
area nssa ........................................................... 19-6
area range .......................................................... 19-7
area stub ............................................................ 19-8
area translate-nssa-to-external ................................ 19-9
area virtual-link .................................................... 19-10
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf as-boundary-router</td>
<td>19-12</td>
</tr>
<tr>
<td>ip ospf authentication-key</td>
<td>19-13</td>
</tr>
<tr>
<td>ip ospf auto-vlink-create</td>
<td>19-14</td>
</tr>
<tr>
<td>ip ospf cost</td>
<td>19-15</td>
</tr>
<tr>
<td>ip ospf dead-interval</td>
<td>19-16</td>
</tr>
<tr>
<td>ip ospf ext-route-metric</td>
<td>19-17</td>
</tr>
<tr>
<td>ip ospf hello-interval</td>
<td>19-18</td>
</tr>
<tr>
<td>ip ospf max-paths</td>
<td>19-19</td>
</tr>
<tr>
<td>ip ospf message-digest-key md5</td>
<td>19-20</td>
</tr>
<tr>
<td>ip ospf packet tracing</td>
<td>19-21</td>
</tr>
<tr>
<td>ip ospf poll interval</td>
<td>19-22</td>
</tr>
<tr>
<td>ip ospf reset-stats</td>
<td>19-23</td>
</tr>
<tr>
<td>ip ospf retransmit-interval</td>
<td>19-24</td>
</tr>
<tr>
<td>ip ospf router-id</td>
<td>19-25</td>
</tr>
<tr>
<td>ip ospf transmit-delay</td>
<td>19-26</td>
</tr>
<tr>
<td>network area</td>
<td>19-27</td>
</tr>
<tr>
<td>passive-interface</td>
<td>19-28</td>
</tr>
<tr>
<td>router ospf</td>
<td>19-29</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>19-30</td>
</tr>
<tr>
<td>show ip ospf database</td>
<td>19-31</td>
</tr>
<tr>
<td>show ip ospf interface</td>
<td>19-32</td>
</tr>
<tr>
<td>show ip ospf neighbor</td>
<td>19-33</td>
</tr>
<tr>
<td>show ip ospf stats</td>
<td>19-34</td>
</tr>
<tr>
<td>show ip ospf virtual-links</td>
<td>19-35</td>
</tr>
<tr>
<td>timers lsa-group-pacing</td>
<td>19-36</td>
</tr>
<tr>
<td>timers spf</td>
<td>19-37</td>
</tr>
</tbody>
</table>

**Chapter 20 — Policy ........................................... 20-1**

- Overview ..................................................... 20-1
- access-list .................................................. 20-2
- ip access-group ............................................. 20-9
- ip access-list .............................................. 20-11
- ip acl-logging .............................................. 20-12
- ip acl-logging logging-interval ...................... 20-13
- show access-group ........................................... 20-14
- show access-list ............................................ 20-15
- show acl-match-timer ....................................... 20-16
- show ip access-list ........................................ 20-17

**Chapter 21 — Port ............................................. 21-1**

- Overview ..................................................... 21-1
- clear port counters ....................................... 21-3
- set port 3com-mapping-table ....................... 21-4
- set port allow-learning .................................. 21-5
- set port auto-flush ........................................ 21-6
- set port auto-negotiation ............................... 21-7
- set port auto-negotiation-duplex-advertisement .................. 21-8
- set port auto-negotiation-flow-control-advertisement .......... 21-9
#### Table of Contents

- **set port auto-negotiation-speed-advertisement** ........................................... 21-10
- **set port auto-vlan-create** ................................................................. 21-11
- **set port category** ................................................................. 21-12
- **set port disable** ........................................................................ 21-13
- **set port duplex** ................................................................. 21-14
- **set port edge admin state** ............................................................... 21-15
- **set port enable** ........................................................................ 21-16
- **set port flow-control** ............................................................... 21-17
- **set port frame-tags** ............................................................... 21-18
- **set port huntgroup** ................................................................. 21-19
- **set port internal-error-shutdown** .................................................... 21-20
- **set port intrusion-trap** ............................................................... 21-21
- **set port intrusion-trap-timer** ....................................................... 21-22
- **set port known-mode** ............................................................... 21-23
- **set port mirror** ................................................................. 21-24
- **set port mirror Fabric_mode2** ......................................................... 21-26
- **set port name** ........................................................................ 21-29
- **set port network-error-detection** ..................................................... 21-30
- **set port pace-priority-mode** ............................................................ 21-32
- **set port point-to-point admin status** ................................................ 21-33
- **set port rate-limit-burst-size** .......................................................... 21-34
- **set port rate-limit-mode** ............................................................. 21-35
- **set port rate-limit-rate** ............................................................... 21-36
- **set port-redundancy** ................................................................. 21-37
- **set port-redundancy name** ............................................................ 21-38
- **set port remote-fault-detect** ............................................................ 21-39
- **set port spanning-tree-mode** ........................................................... 21-40
- **set port speed** ........................................................................ 21-41
- **set port trunking-format** ............................................................... 21-42
- **set port vlan** ........................................................................ 21-43
- **set port vlan-binding-method** ......................................................... 21-44
- **set port vtp-snooping** ................................................................. 21-45
- **show port** ........................................................................ 21-46
- **show port counters** ................................................................. 21-47
- **show port mirror** ................................................................. 21-48
- **show port mirror Fabric_mode2** ....................................................... 21-49
- **show port physical Fabric_mode2** .................................................... 21-50
- **show port status** ................................................................. 21-51
- **show port redundancy** ............................................................... 21-52

**Chapter 22 — Power Cool RAM ................................................................. 22-1**

- **Overview** .................................................................................. 22-1
- **show system fans** ........................................................................ 22-2
- **show system power** ...................................................................... 22-3
- **show system ram** ........................................................................ 22-4
Chapter 23 — 80-Series QoS ........................................... 23-1
  Overview ............................................................... 23-1
  access-list ............................................................ 23-2
  reset port queue counters ........................................ 23-9
  set aft entry ......................................................... 23-11
  set diffserv plp ..................................................... 23-15
  set diffserv priority ............................................... 23-16
  set port default-priority ......................................... 23-17
  set port ignore-tag-priority ...................................... 23-19
  set port mask-diffserv ............................................ 23-21
  set port police ..................................................... 23-23
  set port queue service cbq ....................................... 23-25
  set port queue service cbwfq ..................................... 23-26
  set port queue service strict-priority .......................... 23-28
  set port queue service wfq ....................................... 23-29
  set port use-diffserv .............................................. 23-30
  show diffserv table ............................................... 23-32
  show port ........................................................... 23-33
  show port police .................................................. 23-34
  show port queue buffer .......................................... 23-35
  show port queue counters ........................................ 23-36
  show port queue service ......................................... 23-38

Chapter 24 — RADIUS. .................................................. 24-1
  Overview ............................................................... 24-1
  set radius authentication ......................................... 24-2
  set radius authentication group .................................. 24-3
  set radius authentication realm .................................. 24-4
  set radius authentication retry-number ......................... 24-5
  set radius authentication retry-time ............................ 24-6
  set radius authentication server .................................. 24-7
  set radius authentication source-ip .............................. 24-8
  set radius authentication switch-service-type-required ........ 24-9
  set radius authentication udp-port ............................... 24-10
  show radius authentication ....................................... 24-11

Chapter 25 — SNMP ...................................................... 25-1
  Overview ............................................................... 25-1
  snmp-server ........................................................ 25-2
  snmp-server atm-community ....................................... 25-3
  snmp-server community ............................................ 25-4
  snmp-server contact ............................................... 25-5
  snmp-server engineid .............................................. 25-6
  snmp-server group ................................................. 25-7
  snmp-server location .............................................. 25-9
  snmp-server notify ................................................ 25-10
  snmp-server password ............................................. 25-11
Table of Contents

<table>
<thead>
<tr>
<th>Command Reference Guide for the Avaya P580 and P882 Multiservice Switches, v6.1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter 26 — SSH</strong></td>
</tr>
<tr>
<td>snmp-server user</td>
</tr>
<tr>
<td>snmp-server view</td>
</tr>
<tr>
<td>show snmp</td>
</tr>
<tr>
<td>show snmp community</td>
</tr>
<tr>
<td>show snmp engineid</td>
</tr>
<tr>
<td>show snmp group</td>
</tr>
<tr>
<td>show snmp user</td>
</tr>
<tr>
<td>show snmp view</td>
</tr>
<tr>
<td>clear ssh</td>
</tr>
<tr>
<td>ip ssh</td>
</tr>
<tr>
<td>ssh</td>
</tr>
<tr>
<td>ssh keygen</td>
</tr>
<tr>
<td>ssh timeout</td>
</tr>
<tr>
<td>show ssh</td>
</tr>
</tbody>
</table>

| **Chapter 27 — SSL**   | **27-1** |
| clear ssh              | 27-2   |
| ip https               | 27-3   |
| show ssl cert          | 27-4   |
| show ssl certreq       | 27-5   |
| show ssl ciphers       | 27-6   |
| show ssl config        | 27-7   |
| ssl backcert           | 27-8   |
| ssl certreq            | 27-9   |
| ssl restart            | 27-10  |
| ssl selfcert           | 27-11  |
| show vlan              | 27-12  |

| **Chapter 28 — Rapid Spanning Tree Protocol** | **28-1** |
| overview               | 28-1   |
| set port edge admin state | 28-2 |
| set port point-to-point admin status | 28-3 |
| set port spanning-tree-mode | 28-4 |
| set port spantree force-protocol-migration | 28-5 |
| set port spantree priority | 28-6 |
| set spantree            | 28-7   |
| set spantree config     | 28-8   |
| set spantree default-path-cost | 28-9 |
| set spantree fwwdelay   | 28-10  |
| set spantree hello      | 28-11  |
| set spantree hold-count | 28-12  |
| set spantree maxage     | 28-13  |
| set spantree portcost   | 28-14  |
| set spantree priority   | 28-15  |
| set spantree version    | 28-16  |
show spantree ................................................................. 28-26
show spantree blocked .................................................. 28-28
show spantree config .................................................... 28-29
show spantree port ....................................................... 28-30
show spantree version .................................................. 28-32

Chapter 29 — Switch Fabric ................................. 29-1

Overview ............................................................... 29-1
set fabric configure-redundant-hardware ....................... 29-2
set fabric enable-redundant-element ......................... 29-3
set fabric toggle-active-controller ......................... 29-4
show fabric status ................................................... 29-5

Chapter 30 — System ........................................... 30-1

Overview ............................................................... 30-1
boot system flash ..................................................... 30-4
calendar set .......................................................... 30-5
clear utilization high-threshold ................................. 30-6
clear utilization monitoring ........................................ 30-7
clear utilization threshold-event ............................... 30-8
clock set .............................................................. 30-9
clock summer-time recurring ...................................... 30-10
clock timezone ....................................................... 30-11
copy ................................................................. 30-12
copy <filename> running-config .................................. 30-13
copy <filename> startup-config ................................... 30-14
copy <filename_opt_path> tftp ................................ 30-15
copy card-image bootflash ......................................... 30-16
copy card-image flash .............................................. 30-17
copy <filename1> pcmcia <filename2> ......................... 30-18
copy pcmcia <filename1> <filename2> ......................... 30-19
copy running-config ................................................ 30-20
copy running-config startup-config ......................... 30-21
copy running-config tftp ........................................ 30-22
copy startup-config ............................................... 30-23
copy startup-config running-config ......................... 30-24
copy startup-config tftp ........................................ 30-25
copy tftp ............................................................ 30-26
copy tftp bootflash ................................................ 30-27
copy tftp flash ....................................................... 30-28
copy tftp pcmcia .................................................... 30-29
copy tftp running-config ......................................... 30-30
copy tftp startup-config ......................................... 30-31
cpu_redundancy console ........................................... 30-32
cpu_redundancy hello-interval .................................. 30-33
cpu-redundancy mac-prefix .................................... 30-34
cpu_redundancy mac-prefix .................................... 30-35
delete pcmcia ......................................................... 30-36
## Table of Contents

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir</td>
<td>30-37</td>
</tr>
<tr>
<td>erase</td>
<td>30-38</td>
</tr>
<tr>
<td>erase legacy-configs</td>
<td>30-39</td>
</tr>
<tr>
<td>erase scripts</td>
<td>30-40</td>
</tr>
<tr>
<td>erase startup-config</td>
<td>30-41</td>
</tr>
<tr>
<td>get 48_port_mode</td>
<td>30-42</td>
</tr>
<tr>
<td>get Fabric_mode</td>
<td>30-43</td>
</tr>
<tr>
<td>hostname</td>
<td>30-44</td>
</tr>
<tr>
<td>ip http help server</td>
<td>30-45</td>
</tr>
<tr>
<td>nvram initialize</td>
<td>30-46</td>
</tr>
<tr>
<td>pcmcia initialize</td>
<td>30-47</td>
</tr>
<tr>
<td>reload</td>
<td>30-48</td>
</tr>
<tr>
<td>reset</td>
<td>30-49</td>
</tr>
<tr>
<td>secure-mode</td>
<td>30-50</td>
</tr>
<tr>
<td>set 48_port_mode</td>
<td>30-51</td>
</tr>
<tr>
<td>set debug</td>
<td>30-52</td>
</tr>
<tr>
<td>set Fabric_mode</td>
<td>30-53</td>
</tr>
<tr>
<td>set utilization high-threshold</td>
<td>30-54</td>
</tr>
<tr>
<td>set utilization monitoring</td>
<td>30-56</td>
</tr>
<tr>
<td>set utilization threshold-event</td>
<td>30-57</td>
</tr>
<tr>
<td>setup</td>
<td>30-58</td>
</tr>
<tr>
<td>show boot</td>
<td>30-59</td>
</tr>
<tr>
<td>show calendar</td>
<td>30-60</td>
</tr>
<tr>
<td>show clock</td>
<td>30-61</td>
</tr>
<tr>
<td>show cpu</td>
<td>30-62</td>
</tr>
<tr>
<td>show cpu_redundancy</td>
<td>30-63</td>
</tr>
<tr>
<td>show file_name</td>
<td>30-64</td>
</tr>
<tr>
<td>show flash</td>
<td>30-65</td>
</tr>
<tr>
<td>show running-config</td>
<td>30-66</td>
</tr>
<tr>
<td>show secure-mode</td>
<td>30-67</td>
</tr>
<tr>
<td>show sntp</td>
<td>30-68</td>
</tr>
<tr>
<td>show startup-config</td>
<td>30-69</td>
</tr>
<tr>
<td>show time zone</td>
<td>30-70</td>
</tr>
<tr>
<td>show utilization results</td>
<td>30-71</td>
</tr>
<tr>
<td>show utilization settings</td>
<td>30-72</td>
</tr>
<tr>
<td>show version</td>
<td>30-73</td>
</tr>
</tbody>
</table>

### Chapter 31 — Temperatures ................................ 31-1

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>31-1</td>
</tr>
<tr>
<td>clear temperatures</td>
<td>31-2</td>
</tr>
<tr>
<td>set temperature (shutdown)</td>
<td>31-3</td>
</tr>
<tr>
<td>set temperature (warning)</td>
<td>31-4</td>
</tr>
<tr>
<td>show temperatures</td>
<td>31-6</td>
</tr>
</tbody>
</table>
Chapter 32 — User Interface ........................................... 32-1

- Overview .......................................................... 32-1
- configure ......................................................... 32-3
- connect .......................................................... 32-4
- custom-access-type ............................................ 32-5
- disable .......................................................... 32-7
- enable ............................................................ 32-8
- end ............................................................... 32-9
- exit ............................................................... 32-10
- help .............................................................. 32-11
- length .......................................................... 32-12
- password ....................................................... 32-13
- set custom-access-type ...................................... 32-14
- set debug ....................................................... 32-16
- set login ......................................................... 32-17
- show custom-access-type .................................... 32-18
- show history ..................................................... 32-19
- show login ....................................................... 32-20
- show sessions .................................................. 32-21
- show username .................................................. 32-22
- telnet ............................................................ 32-23
- terminal databits .............................................. 32-24
- terminal flowcontrol ......................................... 32-25
- terminal length ................................................ 32-26
- terminal output pause ....................................... 32-27
- terminal parity ................................................ 32-28
- terminal speed ................................................ 32-29
- terminal stopbits .............................................. 32-30
- terminal width ................................................ 32-31
- username ....................................................... 32-32
- width ........................................................... 32-34

Chapter 33 — VLAN ..................................................... 33-1

- Overview .......................................................... 33-1
- set 3com-mapping-table ...................................... 33-2
- set vlan .......................................................... 33-3
- set vlan (frame format) ...................................... 33-4
- set vlan \<vlan-id> \<mod-swport-range> \ ............... 33-5
- set vtp-snooping domain ..................................... 33-7
- show 3com-mapping-table .................................... 33-8
- show vlan ........................................................ 33-9
- show vtp-snooping configure ................................ 33-10
### Chapter 34 — VRRP

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>34-1</td>
</tr>
<tr>
<td>router vrrp</td>
<td>34-2</td>
</tr>
<tr>
<td>ip vrrp</td>
<td>34-3</td>
</tr>
<tr>
<td>ip vrrp (vr-id)</td>
<td>34-4</td>
</tr>
<tr>
<td>ip vrrp (auth-key)</td>
<td>34-5</td>
</tr>
<tr>
<td>ip vrrp (override)</td>
<td>34-6</td>
</tr>
<tr>
<td>ip vrrp (preempt)</td>
<td>34-7</td>
</tr>
<tr>
<td>ip vrrp (priority)</td>
<td>34-8</td>
</tr>
<tr>
<td>ip vrrp (timer)</td>
<td>34-9</td>
</tr>
<tr>
<td>show ip vrrp</td>
<td>34-10</td>
</tr>
</tbody>
</table>

### Index

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IN-1</td>
<td></td>
</tr>
</tbody>
</table>
1 Overview

This chapter describes:

- Command Mode Summaries
- Entering and Exiting the Command Modes
- Basic Functions
- Accessing the CLI

Command Mode Summaries

The CLI for the Avaya P580 and P882 Multiservice switches consists of various command modes. The commands you can enter depend on the mode you are in. Each command mode has a distinct prompt. Table 1-1 describes the main command modes.

To exit command mode, enter `exit`.

Table 1-1. Main Command Mode Summaries

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
<th>To Access</th>
<th>Prompt</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The mode you are in after login. It includes a limited number of commands to display status and statistic information.</td>
<td>Log in.</td>
<td>&gt;</td>
</tr>
<tr>
<td>Privileged</td>
<td>Contains the commands from the User mode and the commands to set operating parameters.</td>
<td>From the User mode, enter <code>enable</code>.</td>
<td>#</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>Commands to configure the system as a whole.</td>
<td>From the Privileged mode, enter <code>configure</code>.</td>
<td>(configure)#</td>
</tr>
</tbody>
</table>
Entering and Exiting the Command Modes

See Table 1-2 for an explanation of how to access and exit the command modes.

Table 1-2. Entering and Exiting the Command Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>To Access</th>
<th>Prompt Displayed</th>
<th>To Exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Log in.</td>
<td>&gt;</td>
<td>Enter exit.</td>
</tr>
<tr>
<td>Privileged</td>
<td>From the User mode, enter enable.</td>
<td>#</td>
<td>Disable or exit returns to the User mode.</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>From the Privileged mode, enter configure.</td>
<td>(configure)#</td>
<td>Exit returns to the Privileged mode.</td>
</tr>
<tr>
<td>Router Configuration</td>
<td>From Global mode, enter router &lt;protocol&gt; (dvmrp, igmp, ospf, rip, or vrrp).</td>
<td>For DVMRP, OSPF, and RIP: (configure router:&lt;protocol&gt;)# For IGMP and VRRP: (configure)#</td>
<td>Exit returns to the Global Configuration mode. End returns to the Privileged mode.</td>
</tr>
<tr>
<td>Interface Configuration</td>
<td>From Global mode, enter interface &lt;interface-name&gt;</td>
<td>(config-if:&lt;interface-name&gt;)#</td>
<td>Exit returns to the Global Configuration mode. End returns to Privileged mode.</td>
</tr>
</tbody>
</table>
Basic Functions

This section provides information about the following switch functions:

- Help
- Command Syntax Conventions
- No Form Commands
- Command Line History Keys

Help

Enter a question mark (?) at the system prompt to display all of the commands in a mode. See Table 1-3 for additional help commands.

Table 1-3. Basic Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>partial-command? (First tokens only -</td>
<td>Lists the commands that begin with the specified character string. There is</td>
<td># m?</td>
</tr>
<tr>
<td>not whole syntax)</td>
<td>no space between the command and question mark.</td>
<td>mtrace</td>
</tr>
<tr>
<td></td>
<td></td>
<td>#</td>
</tr>
<tr>
<td>partial-command &lt;Tab&gt;</td>
<td>Completes a command name.</td>
<td># conf &lt;Tab&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td># configure</td>
</tr>
<tr>
<td>partial-command +</td>
<td>Lists the remaining syntax of all commands that begin with the character</td>
<td>&gt; sh+</td>
</tr>
<tr>
<td></td>
<td>string.</td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>Lists all of the commands for the current mode - complete syntax and help</td>
<td># +</td>
</tr>
<tr>
<td></td>
<td>descriptions.</td>
<td></td>
</tr>
<tr>
<td>?</td>
<td>Lists, if unique, all commands for the current command mode.</td>
<td>(configure)# ?</td>
</tr>
<tr>
<td>command ? (Gives the next token</td>
<td>Lists the command parameters (with a brief explanation, if available).</td>
<td># show ?</td>
</tr>
<tr>
<td>(parameter or keyword))</td>
<td>(parameter or keyword))</td>
<td></td>
</tr>
<tr>
<td></td>
<td>There is a space between the command and the question mark.</td>
<td></td>
</tr>
<tr>
<td>command[parameter] ? (Gives the next</td>
<td>Lists the arguments for a parameter. There is a space between the parameter</td>
<td>(configure)# show ip</td>
</tr>
<tr>
<td>token (parameter or keyword))</td>
<td>and the question mark.</td>
<td>ospf ?</td>
</tr>
</tbody>
</table>
Command Syntax Conventions

See Table 1-4 for an explanation of the command syntax conventions.

Table 1-4. Command Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyword</td>
<td>A command keyword. An alphanumeric string with “.” allowed.</td>
</tr>
<tr>
<td>&lt;parameter&gt;</td>
<td>Variables for which you supply values. A command parameter name, where the name can be anything.</td>
</tr>
<tr>
<td>[optional]</td>
<td>Optional syntax that can be a keyword, parameter, option or any combination thereof.</td>
</tr>
<tr>
<td>{option1</td>
<td>option2}</td>
</tr>
<tr>
<td>[{optional1</td>
<td>optional2}]</td>
</tr>
<tr>
<td>[...,expansion]</td>
<td>Zero or more occurrences of “expansion” are possible. Expansion must be a keyword, parameter, options or any combination thereof. Complete contents of the bracket [...] (“user-ids”) implies that users must be added to the system two at a time.</td>
</tr>
</tbody>
</table>

No Form Commands

Most CLI commands have a no form. In general, the no form disables a feature/function or restores a default for Layer 3 commands. Clear disables the Layer 2 set commands. The Description section of each command describes the no or clear form (if applicable to the command).

Command Line History Keys

The history buffer stores the last 20 commands you have entered. Use these key sequences to recall commands from the history buffer.

Table 1-5. History Buffer Key Sequence

<table>
<thead>
<tr>
<th>Keys</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P</td>
<td>Recalls the most recent command in the history buffer. Repeat the key sequence to recall the other previous commands.</td>
</tr>
<tr>
<td>Ctrl-N</td>
<td>Returns to the more recent command in the history buffer after Ctrl-P is used to recall commands. Repeat the key sequence to recall the other most recent commands.</td>
</tr>
<tr>
<td>Ctrl-C</td>
<td>Enables you to exit from help command (+).</td>
</tr>
</tbody>
</table>
Overview

Accessing the CLI

There are two ways to access the Avaya P550R, P580, P880, and P882 Multiservice Switch CLI:

- Using telnet
- Using a serial interface

Accessing the CLI Using Telnet

To access the CLI using telnet:

1. Obtain the name and password for the user account you will be using.
2. Enter telnet at the prompt.
3. Enter the IP address or host name for the switch to which you are telnetting:

   `telnet <IP address> or hostname`

*Note:* From NT run: `telnet <a.b.c.d>`

Accessing the CLI Using a Serial Interface

To access the CLI using a serial interface (such as HyperTerminal):

1. Obtain the IP address you want to access.
2. Set up a new connection within the serial interface and proceed to connect with the host as directed by the instructions in the specific serial interface software you are using.
Overview

This chapter describes the following commands:

- clear aft instance invalid-learned-entries vlan
- clear aft instance learned-entries vlan
- set aft agetime
- set aft auto-sizing-threshold
- set aft entry
- set aft instance vlan (auto-increment)
- set aft instance vlan (hash-table-size)
- set aft super-agetime
- show aft config
- show aft entry
- show aft instance
clear aft instance invalid-learned-entries vlan

Command Mode
Global Configuration.

Description
Delete all learned entries from a particular AFT instance.

Syntax
clear aft instance invalid-learned-entries vlan { <vlan-id> | name <vlan-name> }

Table 2-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>Specifies the AFT instance associated with the ID of this VLAN.</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>Specifies the AFT instance associated with the name of this VLAN.</td>
</tr>
</tbody>
</table>

Sample Output
The following example clears all invalid learned entries in the AFT instance for the vlan named Default.

(configure) # clear aft instance invalid-learned-entries vlan 1
All Invalid Learned Entries successfully deleted in AFT Instance for Vlan “Default” (vlanID 1).

Systems
clear aft instance learned-entries vlan

Command Mode
Global Configuration.

Description
Delete all learned entries and invalid learned entries from a particular AFT instance.

Syntax
`clear aft instance learned-entries vlan {<vlan-id> | name <vlan-name>}`

Table 2-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td><code>vlan-id</code> - The ID of the VLAN.</td>
</tr>
<tr>
<td>name</td>
<td><code>vlan-name</code> - The name of the VLAN.</td>
</tr>
</tbody>
</table>

Sample Output
The following example clears all learned entries.

```
(configure)# clear aft instance learned-entries vlan 1
All Learned Entries successfully deleted in AFT Instance for Vlan "Default" (vlanID 1).
```

Systems
set aft agetime

Command Mode  Global Configuration.

Description  Sets the AFT age time. The default time is 300 seconds.

Syntax  set aft agetime <age-time-value>

Table 2-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;age-time-value&gt;</td>
<td>Enter the amount of time, in seconds, after which aft entries become invalid. The range is 10–1,000,000 seconds.</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the aft age time to 350 seconds.

(configure)# set aft agetime 350
AFT Age Time successfully set to 350.

set aft auto-sizing-threshold

Command Mode
Global Configuration.

Description
Sets the AFT auto sizing threshold (percentage before auto-incrementing hash tables). The default percentage is 40%.

Syntax
set aft auto-sizing-threshold <threshold-value>

Table 2-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;threshold-value&gt;</td>
<td>Enter the desired percentage full that a hash table must be before it auto-increments itself. Valid values range from 5-90 percent.</td>
</tr>
</tbody>
</table>

Sample Output
The following example sets the aft auto sizing threshold to 60%.

```
(configure)# set aft auto-sizing-threshold 60
AFT Auto Sizing Threshold successfully set to 60%
```

Systems
**set aft entry**

**Command Mode**
Global Configuration.

**Description**
Creates a static AFT entry or modify an existing static or learned AFT entry. The negative form of this command deletes a static or learned aft entry.

**Syntax**

| To Configure: | set aft entry <mac-address> vlan { <vlan-id> | name <vlan-name>} port-binding {filter | forward <mod-port-spec>} [persistence {ageout | permanent}] [priority {normal | high}] [sa-priority {port | aft <entry-priority>} | max-port-aft <entry-priority>] [da-priority {port | aft <entry-priority>} | max-port-aft <entry-priority>] |
| | To Delete: | clear aft entry <mac-address> vlan { <vlan-id> | name <vlan-name>} |

**Table 2-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>The MAC address associated with this entry.</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td>name</td>
<td>The keyword for the VLAN name.</td>
</tr>
<tr>
<td>vlan-name</td>
<td>The name of the VLAN.</td>
</tr>
<tr>
<td>port-binding</td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>filter</strong> - AFT entries with a filter port binding are dropped when received.</td>
</tr>
<tr>
<td></td>
<td>• <strong>forward</strong> - The port from which the mac address is forwarded.</td>
</tr>
<tr>
<td></td>
<td>• <strong>mod-port-spec</strong> - Specifies a particular port.</td>
</tr>
<tr>
<td>persistence</td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ageout</strong> - The entry is aged as per-learned entries.</td>
</tr>
<tr>
<td></td>
<td>• <strong>permanent</strong> - The entry is not aged out.</td>
</tr>
</tbody>
</table>

1 of 2
### Table 2-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>normal</strong> - The AFT entry has normal priority.</td>
</tr>
<tr>
<td></td>
<td>- <strong>high</strong> - The AFT entry has high priority.</td>
</tr>
<tr>
<td>sa-priority port</td>
<td>Uses the priority of the physical port, Cisco ISL tag, or 802.1p tag to determine the layer 2 priority of frames.</td>
</tr>
<tr>
<td>sa-priority aft</td>
<td>Uses the priority that is assigned to the source MAC address in the Address Forwarding Table (AFT) to determine the layer 2 priority of frames.</td>
</tr>
<tr>
<td><code>&lt;entry-priority&gt;</code></td>
<td>The priority that you want to assign to the source MAC address. Enter a number between 0 and 7. This priority is stored in the AFT entry for the MAC address that you specify.</td>
</tr>
<tr>
<td>sa-priority max-port-aft</td>
<td>Determines the priority of a frame by using the higher of the:</td>
</tr>
<tr>
<td></td>
<td>- Physical port priority or tag priority</td>
</tr>
<tr>
<td></td>
<td>- Source MAC address priority</td>
</tr>
<tr>
<td>da-priority port</td>
<td>Uses the priority of the physical port, Cisco ISL tag, 802.1p tag, or source MAC address to determine the layer 2 priority of frames.</td>
</tr>
<tr>
<td>da-priority aft</td>
<td>Uses the priority that is assigned to the destination MAC address in the AFT to determine the priority of the frame.</td>
</tr>
<tr>
<td><code>&lt;entry-priority&gt;</code></td>
<td>The priority that you want to assign to the destination MAC address. Enter a number between 0 and 7.</td>
</tr>
<tr>
<td>da-priority max-port-aft</td>
<td>Determines the priority of the frame by using the higher of the:</td>
</tr>
<tr>
<td></td>
<td>- Physical port priority or tag priority</td>
</tr>
<tr>
<td></td>
<td>- Destination MAC address priority</td>
</tr>
</tbody>
</table>
### Sample Output

<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set an aft entry on “Default” vlan, with a port binding option of “forward,” a persistence option of “ageout” and a “normal” priority</td>
<td>set aft entry 44:44:44:44:44:44 vlan name “Default” port-binding forward 3/1 persistence ageout priority normal</td>
</tr>
<tr>
<td>• Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.</td>
<td>set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 sa-priority aft 7</td>
</tr>
<tr>
<td>• Forward frames that have a source or destination MAC address of 00:00:00:00:00:55.</td>
<td></td>
</tr>
<tr>
<td>• Assign a priority of 7 to frames that have a source MAC address of 00:00:00:00:00:55.</td>
<td></td>
</tr>
<tr>
<td>• Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.</td>
<td>set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 sa-priority max-port-aft 5</td>
</tr>
<tr>
<td>• Forward frames that have a source or destination MAC address of 00:00:00:00:00:55.</td>
<td></td>
</tr>
<tr>
<td>• Associate a priority of 5 with the source MAC address of 00:00:00:00:00:55.</td>
<td></td>
</tr>
<tr>
<td>• Assign the higher of the port priority, tag priority, or source MAC address priority (5) to frames that have a source MAC address of 00:00:00:00:00:55.</td>
<td></td>
</tr>
</tbody>
</table>
### Systems


<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
</table>
| • Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.  
• Forward frames that have a source or destination MAC address of 00:00:00:00:00:55.  
• Assign a priority of 7 to packets that have a destination MAC address of 00:00:00:00:00:55. | set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 da-priority aft 7 |
| • Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.  
• Forward frames that have a source or destination MAC address of 00:00:00:00:00:55.  
• Associate a priority of 5 with the destination MAC of address 00:00:00:00:00:55.  
• Assign the higher of the port priority, tag priority, or destination MAC address priority (5) to frames that have a destination MAC address of 00:00:00:00:00:55. | set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 da-priority max-port-aft 5 |
**set aft instance vlan (auto-increment)**

**Command Mode**
Global Configuration.

**Description**
Sets the auto-increment flag for a particular VLAN’s AFT instance.

**Syntax**
```
set aft instance vlan {<vlan-id> | name <vlan-name>} auto-increment-ht-size {true | false}
```

**Table 2-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>The AFT instance associated with the VLAN.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td>name</td>
<td>The keyword for the VLAN name.</td>
</tr>
<tr>
<td>vlan-name</td>
<td>The name of the vlan.</td>
</tr>
<tr>
<td>auto-increment-ht-size</td>
<td>Specify whether or not the hash table should auto-increment itself. The options are:</td>
</tr>
<tr>
<td></td>
<td>true - The hash table auto-increments itself.</td>
</tr>
<tr>
<td></td>
<td>false - The hash table does not auto-increment itself.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the auto-increment flag for the aft instance vlan named “Default” to false, which means that the hash table does not auto-increment itself.

```
(configure)# set aft instance vlan name 'Default'
auto-increment-ht-size false
```

AFT Instance Hash Table Auto-Increment for Vlan "Default" (vlanID 1) successfully set to false

**Systems**
set aft instance vlan (hash-table-size)

**Command Mode**
Global Configuration.

**Description**
Sets the hash table size for a particular VLAN’s AFT instance.

**Syntax**
```
set aft instance vlan { <vlan-id> | name <vlan-name> } hash-table-size { 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 4096 | 8192 }
```

**Table 2-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>The AFT instance associated with the VLAN.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>- The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td>name</td>
<td>The keyword for the VLAN name.</td>
</tr>
<tr>
<td>vlan-name</td>
<td>- The name of the vlan.</td>
</tr>
<tr>
<td>hash-table-size</td>
<td>Specifies the hash table size. The table size specified must be one of the</td>
</tr>
<tr>
<td></td>
<td>following (all values are power of 2):</td>
</tr>
<tr>
<td></td>
<td>16</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the AFT instance vlan named “default” hash table size to 2048.

```
(configure)# set aft instance vlan name “Default” hash-table-size 2048
AFT Instance Hash Table Size for Vlan “Default” (vlanID 1) successfully set to 2048
```

**Systems**
set aft super-agetime

Command Mode
Global Configuration.

Description
Sets the AFT super age time. The default is seven (7) days.

Syntax
set aft super-agetime <super-age-time-value>

Sample Output
The following example sets the aft super age time to 8 days.

(configure)# set aft super-agetime 8
AFT Super Age Time successfully set to 8

Systems

Table 2-8. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;super-age-time-value&gt;</td>
<td>Enter the amount of time, in days, after which invalid aft entries are removed. The range is 1-30 days.</td>
</tr>
</tbody>
</table>
show aft config

Command Mode  User.

Description      Displays the AFT’s global configuration.

Syntax           show aft config

Sample Output    The following example displays the aft manager configuration table.

> show aft config
AFT Manager Configuration:
-----------------------------------------
Age Time: 300
Super Age Time: 7

AFT PLE Configuration:
-----------------------------------------
Initial Hash Table Size: 1024
Utilization Threshold: 40%
Bkt Size To Trig Util: 32
HT Size Mult To Trig Util: 12

show aft entry

Command Mode     User.

Description      Performs a search for all of the AFT entries that matches the criteria specified in the command.

Syntax           show aft entry [mac <wildcard-mac-address>] [vlan {<vlan-id> | name <vlan-name>}] [port-binding {cpu | filter | forward [<mod-port-spec>]}] [status {learned | management | self | multicast}]

Table 2-9. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac</td>
<td>The MAC address associated with this entry.</td>
</tr>
<tr>
<td>wildcard-mac-address</td>
<td>the wildcard is indicated by a single asterisk (*) before the MAC address.</td>
</tr>
<tr>
<td>vlan</td>
<td>&lt;vlan-id&gt; - the ID of the VLAN.</td>
</tr>
<tr>
<td>name</td>
<td>&lt;vlan-name&gt; - the name of the VLAN.</td>
</tr>
<tr>
<td>port-binding</td>
<td>Specifies the binding of the entry to be displayed. VLAN.</td>
</tr>
<tr>
<td>cpu</td>
<td>Displays entries bound to the CPU.</td>
</tr>
<tr>
<td>filter</td>
<td>Displays filtered entries.</td>
</tr>
<tr>
<td>forward</td>
<td>Displays forwarding entries.</td>
</tr>
<tr>
<td>mod-port-spec</td>
<td>Applies only to forwarding entries and specifies the ports for</td>
</tr>
<tr>
<td></td>
<td>which forwarding entries are to be displayed.</td>
</tr>
<tr>
<td>status</td>
<td>Displays the following entries:</td>
</tr>
<tr>
<td></td>
<td>• learned - Displays learned entries only</td>
</tr>
<tr>
<td></td>
<td>• management - Displays management entries only</td>
</tr>
<tr>
<td></td>
<td>• self - Displays self entries</td>
</tr>
<tr>
<td></td>
<td>• multicast - Displays multicast entries only</td>
</tr>
</tbody>
</table>
Sample Output

The following example display the aft entry table.

> show aft entry

AFT Entries matching search criteria: "All Entries"

===============================================
MAC Address  Port  Valid VlanID Priority Persistence Status
01:80:C2:00:00:00  cpu  valid  2  high  permanent  self
01:80:C2:00:00:01  cpu  valid  2  high  permanent  self
01:80:C2:00:00:02  filter valid  2  normal  permanent  self
01:80:C2:00:00:03  filter valid  2  normal  permanent  self
01:80:C2:00:00:04  filter valid  2  normal  permanent  self

Systems

show aft instance

Command Mode

User.

Description
Displays the AFT instance for a particular VLAN or show all AFT instances for all VLANs. If no VLAN parameter is specified, all instances show on the switch.

Syntax
show aft instance [vlan {<vlan-id> | name <vlan-name> }]

Sample Output
The following example displays the aft instance configuration table.

> show aft instance
AFT Instance Configuration:

--------------------------------------------
Instance for Vlan “Default” (vlanID 1)
 AutoSizeHT:            true
 UseConfHTsize:         false
 KeepInvalidInCol:      false
 UseInvalidInBktSizing: true
 KeepInvalidInBkt:      false
 ConfigHTsize:          1024
Instance for Vlan “Discard” (vlanID 4097)
 AutoSizeHT:            false
 UseConfHTsize:         false
 KeepInvalidInCol:      false
 UseInvalidInBktSizing: true
 KeepInvalidInBkt:      false
 ConfigHTsize:          1

Systems
3 Appletalk

Overview

This chapter describes the following commands:

- appletalk access-group
- appletalk access-list
- appletalk address
- appletalk admin-state
- appletalk cable-range
- appletalk echo
- appletalk mac-format
- appletalk routing
- appletalk static cable-range
- appletalk vlan
- appletalk zone
- clear appletalk arp
- clear appletalk route
- clear appletalk traffic
- ping appletalk
- show appletalk access-lists
- show appletalk arp
- show appletalk globals
- show appletalk interface
- show appletalk nbp
- show appletalk route
- show appletalk static cable-range
- show appletalk traffic
- show appletalk zone
**appletalk access-group**

**Command Mode**  
Interface Configuration.

**Description**  
Assign an access list to an Appletalk interface. The no form of this command removes the access list from the interface.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>appletalk access-group &lt;access-list-number&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no appletalk access-group &lt;access-list-number&gt;</td>
</tr>
</tbody>
</table>

**Table 3-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list-number&gt;</td>
<td>A decimal value that specifies the identifier of the access list. This is a number between 600 and 663.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example enables access-group 625 to an Appletalk interface.

```
(config-if:serial0)# appletalk access-group 625
```

**Systems**  
appletalk access-list

**Command Mode**  
Global Configuration.

**Description**  
Creates an Appletalk Access List. The no form of this command removes an Appletalk Access List. The default is to permit all zones and all NBP objects.

The access list applies to either an Appletalk zone name or to the object portion of an NBP entity. To delete a zone from the zone list, delete the static route first.

**Syntax**

| To Enable: | appletalk access-list <access-list-number> {deny | permit} { {nbp | zone} <string> | additional-zones | additional-nbps} |
|------------|----------------------------------------------------------------------------------------------------------------------------------|
| To Disable: | [no] appletalk access-list <access-list-number> |

**Table 3-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list-number&gt;</td>
<td>The identifier (in decimal) of the access list.</td>
</tr>
<tr>
<td></td>
<td>The access-list-number for nbp must be between 600 and 631.</td>
</tr>
<tr>
<td></td>
<td>The access-list-number for zone must be between 632 and 663.</td>
</tr>
<tr>
<td>deny</td>
<td>Prevents access when conditions match. Specifying deny denies access if the conditions are matched.</td>
</tr>
<tr>
<td>permit</td>
<td>Allows access when conditions match. Specifying permit permits access if the conditions are matched.</td>
</tr>
<tr>
<td>nbp</td>
<td>Applies the access-list to the &lt;string&gt; field of Appletalk Naming Binding Protocol (NBP) entities.</td>
</tr>
<tr>
<td>zone</td>
<td>Applies the access-list to Appletalk Zone names.</td>
</tr>
<tr>
<td>&lt;string&gt;</td>
<td>The name of the zone or NBP object to which this entry applies.</td>
</tr>
</tbody>
</table>
### Table 3-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>additional-zones</td>
<td>Additional zone names. This keyword defines the default action to take for access check, which apply to zones.</td>
</tr>
<tr>
<td>additional-nbps</td>
<td>Additional Naming Binding Protocol entities. This keyword defines the default action to take for access checks, which apply to nbp.</td>
</tr>
</tbody>
</table>

### Sample Output

The following example disables Appletalk access list 630.

```
(configuration)# no appletalk access-list 630
```

### Systems

appletalk address

Command Mode  Interface Configuration.

Description  Configure an Appletalk Phase I Address for an interface. The no form of this command removes the Appletalk interface itself.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>appletalk address (&lt;\text{network.node}\rangle)</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] appletalk address</td>
</tr>
</tbody>
</table>

Table 3-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| \(<\text{network.node}\rangle\) | • **network** - A 16-bit network number between 0 and 66279.  
  • **node** - An 8-bit node number between 0 and 254.  
  Separate the network and node values with a period. When omitted, the Appletalk address defaults to 0.0. |

appletalk admin-state

Command Mode

Interface Configuration.

Description

Set the administrative state of an Appletalk Interface. The default value is up.

Syntax

appletalk admin-state {up | down}

Table 3-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{up</td>
<td>down}</td>
</tr>
<tr>
<td></td>
<td>• up - The administrative state of the interface is active.</td>
</tr>
<tr>
<td></td>
<td>• down - The administrative state of the interface is inactive.</td>
</tr>
</tbody>
</table>

Sample Output

The following example sets the Appletalk administrative state to down.

(config-if:serial0)# appletalk admin-state down

Systems

appletalk cable-range

Command Mode  Interface Configuration.
Description  Configure a cable range for an Appletalk Phase II for an interface. The no form of this command disables Appletalk for this interface.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>appletalk cable-range &lt;cable-range&gt; [&lt;network.node&gt;]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] appletalk cable-range</td>
</tr>
</tbody>
</table>

Sample Output  The following example configures a cable range of 222-224 for the Appletalk interface on serial port 0.

    (config-if:serial0)# appletalk cable-range 222.244


Table 3-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;cable-range&gt;</td>
<td>An optional parameter to indicate the range of the Appletalk network values to be used on this interface. Specify start and end values between 0 and 65279 and separate the values with a hyphen. The starting network number must be less than the ending network number. When &lt;cable-range&gt; is omitted, the interface tries to configure the Appletalk network and obtains its configuration from another Appletalk router.</td>
</tr>
</tbody>
</table>
| <network.node> | The Appletalk network address to assign to the interface. When <network.node> is omitted, the Appletalk address defaults to 0.0.  
  • network - A 16-bit network number between 0 and 66279.  
  • node - An 8-bit node number between 0 and 254. |
**appletalk echo**

**Command Mode**  
Privileged.

**Description**  
Send an Appletalk echo request to a specified Appletalk node.

**Syntax**  
appletalk echo <network.node>

**Table 3-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;network.node&gt;</td>
<td>• <strong>network</strong> - The DDP network address of the Appletalk device.</td>
</tr>
<tr>
<td></td>
<td>• <strong>node</strong> - The DDP node address of the Appletalk device.</td>
</tr>
</tbody>
</table>

**Systems**  
appletalk mac-format

Command Mode  Interface Configuration.

Description  Sets which Appletalk Interface MAC format is to be used. The default value is snap. The no form of this command resets the MAC format for the interface to the default value.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
</tr>
</thead>
<tbody>
<tr>
<td>appletalk mac-format {ethv2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To Restore Default:</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] appletalk mac-format</td>
</tr>
</tbody>
</table>

Table 3-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ethv2</td>
<td>snap}</td>
</tr>
<tr>
<td></td>
<td>• snap - Subnetwork Access Protocol.</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the Appletalk Interface MAC format to ethv2.

(config-if:serial0)# appletalk mac-format ethv2

appletalk routing

**Command Mode**
Global Configuration.

**Description**
Enables Appletalk routing. The no form of this command disables Appletalk routing. The default for Appletalk routing is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>appletalk routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] appletalk routing</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables Appletalk routing.

```
(configuration)# appletalk routing
```

**Systems**
appletalk static cable-range

Command Mode
Global Configuration.

Description
Creates an Appletalk static route. The no form of this command removes the static route itself, or only removes a zone from the static route if the zone name is supplied.

Syntax

| To Enable: | appletalk static cable-range <cable-range> to <network.node> [floating] zone <zone-name> |
| To Disable: | [no] appletalk static cable-range <cable-range> to <network.node> |

Table 3-8. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;cable-range&gt;</td>
<td>The range of Appletalk network values to be used for this static route. Specify start and end values, in decimal, between 0 and 65279 and separate the values with a hyphen. The starting network number must be less than the ending network number. The next hop Appletalk router is specified via the network.node parameter.</td>
</tr>
</tbody>
</table>
| <network.node> | Specifies the Appletalk Network Address of the next hop to the destination network. (Both numbers are in decimal.)  
  - **network** - A 16-bit network number between 0 and 66279.  
  - **node** - An 8-bit node number between 0 and 254. |
| [floating]   | Specifies that a dynamic route update for this network can replace the route entry created by this command.  
The floating argument is optional. If supplied, the route defined via this command may be overwritten by an Appletalk routing update. The default is to ignore Appletalk route updates for this cable range. |
| <zone-name>  | A zone name to be associated with this destination.  
  When the keyword zone and the zone-name are omitted, the static route is removed. |
### Sample Output
The following example creates a static route to a remote router whose address is 1.5 on the remote network 110-120 in the remote zone “adams”.

```
(configure)# appletalk static cable-range 110-120 to 1.5 zone adams
```

### Systems
**appletalk vlan**

**Command Mode**  Interface Configuration.

**Description**  Assigns the Appletalk interface to a VLAN. The no form of this command resets the VLAN to the discard VLAN, which is the default value.

**Syntax**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Enable:</strong></td>
<td>appletalk vlan { &lt;vlan-id&gt;</td>
</tr>
<tr>
<td><strong>To Disable:</strong></td>
<td>[no] appletalk vlan</td>
</tr>
</tbody>
</table>

**Table 3-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The ID of the VLAN Appletalk uses for the interface.</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The name of the VLAN Appletalk uses for the interface.</td>
</tr>
</tbody>
</table>

**Sample Output**  The following example sets Appletalk interface foo2 to VLAN auto50.

```
(config-if: auto50)# appletalk vlan name foo2
```

appletalk zone

Command Mode
Interface Configuration.

Description
Adds an Appletalk zone name to an interface. The no form of this command removes a specifically named zone name from an interface, or all zone names, if no zone name is specified. The first zone added is the default zone. This command can be issued, as needed, to assign additional zone names to an interface.

Syntax

| To Enable:  | appletalk zone [ <zone-name> ] |
| To Disable: | [no] appletalk zone |

Table 3-10. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;zone-name&gt;</td>
<td>The name of the zone you want to add to the interface. The first zone added is the default zone.</td>
</tr>
</tbody>
</table>

Sample Output
The following example adds Appletalk zone “foo2” to the “auto50” interface.

```
(config-if:auto50)# appletalk zone foo2
```

Systems
clear appletalk arp

Command Mode  Global Configuration.

Description  Deletes a single or all entries from the Appletalk ARP and Appletalk Routing tables, and clears the Appletalk counters.

Syntax  clear appletalk arp [<network.node>]

Table 3-11. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;network.node&gt;</td>
<td>• <strong>network</strong> - The Appletalk network address to delete from the AARP table. This is a 16-bit network number in the range 0 to 65279.</td>
</tr>
<tr>
<td></td>
<td>• <strong>node</strong> - An 8-bit node number in the range 0 to 254.</td>
</tr>
<tr>
<td></td>
<td>To delete all dynamic entries, omit the argument. Local and static entries cannot be deleted.</td>
</tr>
</tbody>
</table>

clear appletalk route

**Command Mode**
Global Configuration

**Description**
Delete a single or all Appletalk routing entries from the Appletalk Routing Table.

**Syntax**
clear appletalk route [\(<network>\)]

**Table 3-12. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>(&lt;network&gt;)</td>
<td>The number of the network to which the route provides access. To delete all dynamic entries, omit the argument. Local and static route entries cannot be deleted.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example deletes all entries from the Appletalk Routing table.

(config)# clear appletalk route

**Systems**
clear appletalk traffic

Command Mode  Global Configuration.

Description  Clears the Appletalk counters.

Syntax  clear appletalk traffic

ping appletalk

Command Mode
Privileged.

Description
Sends an Appletalk Echo Request to a specific Appletalk node.

Syntax
ping appletalk <network.node>

Table 3-13. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| <network.node> | • **network** - The DDP network address of the Appletalk device.  
|            | • **node** - The DDP node address of the Appletalk device.       |

Systems
**show appletalk access-lists**

**Command Mode**  
User.

**Description**  
Displays currently defined Appletalk access lists.

**Syntax**  
```
show appletalk access-list
```

**Sample Output**  
The following example displays the Appletalk access list.

```
> show appletalk access-list
Apple Talk Access Lists

<table>
<thead>
<tr>
<th>Index</th>
<th>Type</th>
<th>Operation</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>606</td>
<td>NBP</td>
<td>Deny</td>
<td>Lime</td>
</tr>
<tr>
<td>632</td>
<td>Zone</td>
<td>Permit</td>
<td>Zone700</td>
</tr>
<tr>
<td>633</td>
<td>Zone</td>
<td>Permit</td>
<td>Zone500</td>
</tr>
<tr>
<td>640</td>
<td>Zone</td>
<td>Permit</td>
<td>Area0</td>
</tr>
<tr>
<td>650</td>
<td>Zone</td>
<td>Permit</td>
<td>Zone600</td>
</tr>
</tbody>
</table>
```

**Systems**  
show appletalk arp

**Command Mode**  
User.

**Description**  
List entries in the Appletalk ARP Table.

**Syntax**  
show appletalk arp [all]

**Table 3-14. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[all]</td>
<td>Shows local and broadcast entries, in addition to dynamic entries listed in the Appletalk Arp Table.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example displays the Appletalk arp table.

```
> show appletalk arp
AppleTalk AARP Cache Table
Hardware Address   DDP AddressType  TTL  Interface
F0:0D:04:31:00:31   55.55            Remote 60  at_if2
08:00:07:41:C0:8B   8001.1          Dynamic50 at_if3
```

**Systems**  
# show appletalk globals

**Command Mode**  
User.

**Description**  
Displays information about the router’s Appletalk status.

**Syntax**  
show appletalk globals

**Sample Output**  
The following example displays information about the router’s Appletalk status.

```
> show appletalk globals
   AT Global Statistics
   Apple Talk Routing is enabled
```

**Systems**  
show appletalk interface

Command Mode
User.

Description
Displays Appletalk-related interface settings for a specific interface, or all interfaces when interface-name is omitted.

Syntax
show appletalk interface [brief] [<interface-name>]

Table 3-15. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[brief]</td>
<td>A keyword indicating that only summary information is to be displayed.</td>
</tr>
<tr>
<td>&lt;interface-name&gt;</td>
<td>The name of the interface to display.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays summary information about the Appletalk interface labeled jerry.

```
> show appletalk interface brief jerry
jerry is down, and administratively up
On vlan Internal-Network, is down
Starting Cable Range is 0
Ending Cable Range is 0
DDP Network Number 0
DDP Node Number 0
```

Systems
show appletalk nbp

Command Mode
User.

Description
Displays all Appletalk Name Binding Protocol (NBP) entries.

Syntax
show appletalk nbp

Sample Output
The following example shows the display for the show Appletalk nbp command.

> show appletalk nbp

AppleTalk Name Binding Protocol Table
Index Object : Type@Zone on Interface
  1 PORT_8000.1:Router@Zone8000 on at_if3
  2 PORT_500.1 :Router@Area0 on at_if2
  3 PORT_300.1 :Router@Zone300 on at_if1

Systems
show appletalk route

Command Mode User.

Description Displays the contents of the Appletalk Routing Table.

Syntax show appletalk route [<starting-range>]

Sample Output The following example displays the contents of the Appletalk routing table with “8000” as the starting range.

> show appletalk route 8000
AppleTalk Route Table
Start-End Next Hop Metric State Owner Interface
8000-8001 0.0 0 Good Local at_if3

show appletalk static cable-range

Command Mode User.

Description Displays the static routes that are configured for Appletalk.

Syntax show appletalk static cable-range [<starting-range>]

Table 3-17. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;starting-range&gt;</td>
<td>If the starting range is supplied, the entry corresponding to this specific static route is displayed; otherwise, the entire routing table is displayed.</td>
</tr>
</tbody>
</table>

Sample Output The following example displays all of the Appletalk static routes that are configured.

> show appletalk static cable-range
AppleTalk StaticRoute Table
Start-End Next Hop Metric State Owner Interface
9000-9001 350.50 1 Good Static at_if1

show appletalk traffic

Command Mode
User.

Description
Displays Appletalk Protocol Counters and Statistics.

Syntax
show appletalk traffic

Sample Output
The following example displays the Appletalk protocol counter and statistics.

> show appletalk traffic
AT Traffic Statistics
AppleTalk Traffic Statistics
Echo Req Tx 0 Echo Replies Rcv 0
Echo Req Rcv 0 DDP Output Counter 12
DDP Output Short 0 DDP Output Long 12
DDP Input Counter 0 DDP Fwd Counter 0
DDP Local Counter 0 No Client 0
No Route 0 Too Short 0
Too Long 0 Broadcast Error 0
Short PDU in Error 0 TTL Expired 0
Checksum Error 0 AARP Req Rcv 0
AAPR Replies Rcv 0 AARP Invalid PDU 0
AARP Req Tx 57 AARP Replies Tx 0
RTMP Rq Sent 0 RTMP Rq Rcv 0
RTMP Rsp Sent 0 RTMP Rsp Rcv 0
RTMP RDR Sent 12 RTMP RDR Rcv 0
ZIP Query Sent 0 ZIP Query Rcv 0
ZIP Reply Sent 0 ZIP Reply Rcv 0
ZIP Reply Ext Sent 0 ZIP Reply Ext Rcv 0
ZIP GNI Rq Sent 0 ZIP GNI Rq Rcv 0
ZIP GNI Rsp Sent 0 ZIP GNI Rsp Rcv 0
Config Address Error 0 Config Zone Error 0

Systems
show appletalk zone

Command Mode  User.

Description  Displays the contents of the Appletalk Zone Information Table (ZIT).

Syntax  show appletalk zone [<zone-name>]

Table 3-18. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;zone-name&gt;</td>
<td>The name of the zone corresponding to the entry. When omitted, all entries in the table are displayed.</td>
</tr>
</tbody>
</table>

Sample Output  The following example displays the contents of the Zone1 Appletalk Zone Information table.

> show appletalk zone Zone1
AppleTalk Zone Table
Index Start-End Name
  418     1-10   Zone1
  418   500-600  Zone1

4 Buffering

Overview

This chapter describes the following commands:

- set buffering fabric-port (age-timer)
- set buffering fabric-port (hipri-alloc)
- set buffering fabric-port (hipri-service-ratio)
- set buffering fabric-port (pri-threshold)
- set buffering port (age-timer)
- set buffering port (hipri-alloc)
- set buffering port (hipri-service-ratio)
- set buffering port (pri-threshold)
- show buffering fabric-port
- show buffering port

*Note:* These commands are not supported on 80-Series modules.
set buffering fabric-port (age-timer)

**Command Mode**
Global Configuration.

**Description**
Sets the input or output buffer age timer range for a fabric port. The default age-timer range is 160-320.

**Syntax**
```
set buffering fabric-port <fabric-port-spec> [routing] {input | output} age-timer {160-to-320 | 640-to-1280}
```

**Table 4-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;fabric-port-spec&gt;</code></td>
<td>Enter a particular fabric port or a range of fabric ports on a module.</td>
</tr>
<tr>
<td>[routing]</td>
<td>Set the routing buffer parameters.</td>
</tr>
<tr>
<td>{input</td>
<td>output}</td>
</tr>
<tr>
<td>age-timer</td>
<td>The age-timer ranges are:</td>
</tr>
<tr>
<td></td>
<td>• 160-to-320</td>
</tr>
<tr>
<td></td>
<td>• 640-to-1280</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the buffer age-timer range for fabric port 4/1 to the 640-1280 range.

```
(configure) # set buffering fabric-port 4/1 routing input age-timer 640-to-1280
Buffers for fabric-port 4/1 set.
```

**Systems**
set buffering fabric-port (hipri-alloc)

Command Mode  Global Configuration.

Description  Set the input or output buffer high priority allocation percentage. The default percentage value is 20%.

* Note: The switch must be rebooted for changes to this parameter to take effect.

Syntax  set buffering fabric-port <fabric-port-spec> [routing] {input | output} hipri-alloc {10 | 20 | 30 | 40 | 50}

Table 4-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;fabric-port-spec&gt;</td>
<td>Enter a particular fabric port or a range of fabric ports on a module.</td>
</tr>
<tr>
<td>[routing]</td>
<td>Set the routing buffer parameters.</td>
</tr>
<tr>
<td>{input</td>
<td>output}</td>
</tr>
<tr>
<td>hipri-alloc</td>
<td>The high priority allocation percentage values are: 10, 20, 30, 40, or 50.</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the buffer high priority allocation percentage for fabric port 4/1 to 30%.

    (configure)# set buffering fabric-port 4/2 routing output hipri-alloc 30

set buffering fabric-port (hipri-service-ratio)

**Command Mode** Global Configuration.

**Description** Sets the input or output buffer high priority service ratio for a fabric port. The default ratio is 999-to-1.

**Syntax**

```
set buffering fabric-port <fabric-port-spec> [routing] {input | output} hipri-service-ratio {3-to-1 | 99-to-1 | 999-to-1 | 9999-to-1}
```

**Table 4-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;fabric-port-spec&gt;</code></td>
<td>Enter a particular fabric port or a range of fabric ports on a module.</td>
</tr>
<tr>
<td>[routing]</td>
<td>Set the routing buffer parameters.</td>
</tr>
<tr>
<td>{input</td>
<td>output}</td>
</tr>
<tr>
<td>hipri-service-ratio</td>
<td>The high priority service ratios are: 3-to-1, 99-to-1, 999-to-1, 9999-to-1</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example sets the input buffer high priority service ratio for fabric port 4/1 to 9999-to-1.

```
(configure) # set buffering fabric-port 4/1 routing input hipri-service-ratio 9999-to-1
Buffers for fabric-port 4/1 set.
```

**set buffering fabric-port (pri-threshold)**

**Command Mode**
Global Configuration.

**Description**
Sets the input or output buffer priority threshold for a fabric port. The default value for the priority threshold is 4.

**Syntax**
```
set buffering fabric-port <fabric-port-spec> [routing] {input | output} pri-threshold {1 | 2 | 3 | 4 | 5 | 6 | 7 | all-frames-normal-priority}
```

**Table 4-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;fabric-port-spec&gt;</td>
<td>Enter a particular fabric port or a range of fabric ports on a module.</td>
</tr>
<tr>
<td>[routing]</td>
<td>Set the routing buffer parameters.</td>
</tr>
<tr>
<td>{input</td>
<td>output}</td>
</tr>
<tr>
<td>pri-threshold</td>
<td>The priority thresholds are: 1, 2, 3, 4, 5, 6, 7 or all-frames-normal-priority</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the buffer priority threshold for fabric port 4/1 to 5.

```
(configure)# set buffering fabric-port 4/1 routing output pri-threshold 5
Buffers for fabric-port 4/1 set.
```

**Systems**
set buffering port (age-timer)

**Command Mode**
Global Configuration.

**Description**
Sets the output buffer age timer for a physical port. The default setting is 168.

**Syntax**
set buffering port <mod-port-spec> output age-timer {21 | 42 | 84 | 168 | 336 | 672 | 1340}

**Table 4-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-port-spec&gt;</td>
<td>Specifies the module and the port.</td>
</tr>
<tr>
<td>output</td>
<td>The output buffer.</td>
</tr>
<tr>
<td>age-timer</td>
<td>The values for the age timer are: 21, 42, 84, 168, 336, 672 or 1340.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the output age timer for port 4/1 as 42.

```
(configure)# set buffering port 4/1 output age-timer 42
Buffers for fabric-port 4/1 set.
```

**Systems**
set buffering port (hipri-alloc)

**Command Mode**
Global Configuration.

**Description**
Sets the output buffer high priority allocation percentage for a physical port. The default setting is 20.

**Syntax**
set buffering port <mod-port-spec> output hipri-alloc {10 | 20 | 30 | 40 | 50}

**Table 4-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-port-spec&gt;</td>
<td>Specifies the module and the port.</td>
</tr>
<tr>
<td>output</td>
<td>The output buffer.</td>
</tr>
<tr>
<td>hipri-alloc</td>
<td>The high priority allocation percentages are: 10, 20, 30, 40, or 50.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the output buffer priority allocation percentage for physical port 4/1 to 50.

```
(configure)# set buffering port 4/1 output hipri-alloc 50
Buffers for buffering port 4/1 set.
```

**Systems**
set buffering port (hipri-service-ratio)

Command Mode  
Global Configuration.

Description  
Set the output buffer high priority service ratio for a physical port. The default setting is 1023-to-1.

Syntax  
set buffering port <mod-port-spec> output hipri-service-ratio {1-to-1 | 3-to-1 | 7-to-1 | 15-to-1 | 31-to-1 | 63-to-1 | 127-to-1 | 255-to-1 | 511-to-1 | 1023-to-1 | 2047-to-1 | 4095-to-1 | 8191-to-1 | 16383-to-1 | 32767-to-1}

Sample Output  
The following example sets the buffer high priority service ratio for physical port 4/1 to 15-to-1.

(configure)# set buffering port 4/1 output hipri-service-ratio 15-to-1
Buffers for port 4/1 set.

Systems  
set buffering port (pri-threshold)

Command Mode      Global Configuration.

Description       Sets the output buffer priority threshold for a physical port. The default setting is 4.

Syntax            set buffering port <mod-port-spec> output pri-threshold {1 | 2 | 3 | 4 | 5 | 6 | 7 | all-frames-normal-priority}

Sample Output     The following example sets the output buffer priority threshold for physical port 4/1 to 5.

                    (configure)# set buffering port 4/1 output pri-threshold 5


<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-port-spec&gt;</td>
<td>Specifies the module and the port.</td>
</tr>
<tr>
<td>output</td>
<td>The output buffer.</td>
</tr>
<tr>
<td>pri-threshold</td>
<td>The priority thresholds are: 1, 2, 3, 4, 5, 6, 7 or all-frames-normal-priority.</td>
</tr>
</tbody>
</table>
show buffering fabric-port

**Command Mode**  
User.

**Description**  
Displays the buffering configuration and statistics for a fabric port.

**Syntax**  
show buffering fabric-port [<fabric-port-spec> [,...,<fabric-port-spec>]]

**Table 4-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;fabric-port-spec&gt;</td>
<td>Specifies a fabric port.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example displays the buffering configuration and statistics for fabric-port 4/1-4/10

```plaintext
> show buffering fabric-port 4/1-4/10

Fabric Port:4/1-4/8    Input Buffer    Output Buffer
----------------------------------------------------------------
Memory(KB): 256        496
Age Timer(ms): 160-to-320 160-to-320
HiPri Allocation(%) run:20 20
HiPri Allocation(%) cfg:20 20
Priority Threshold: 4 4
High Pri Service Ratio: 999-to-1 999-to-1
High Overflow Drops: 0 0
Overflow Drops: 0 0
High Stale Drops: 0 0
Stale Drops: 0 0
Congestion Drops: 0 0

```

**Systems**  
show buffering port

**Command Mode**  
User.

**Description**  
Displays the buffer configuration and statistics for a physical port.

**Syntax**  
show buffering port [<mod-port-spec>[,<mod-port-spec>]]

**Sample Output**  
The following example displays the buffer configuration and statistics for physical port 6/19.

> show buffering port 6/19

<table>
<thead>
<tr>
<th>Physical Port: 6/19</th>
<th>Input Buffer</th>
<th>Output Buffer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory):</td>
<td>16</td>
<td>116</td>
</tr>
<tr>
<td>Age Timer):</td>
<td>-</td>
<td>168</td>
</tr>
<tr>
<td>HiPri Allocation(%) run:</td>
<td>-</td>
<td>20</td>
</tr>
<tr>
<td>HiPri Allocation(%) cfg:</td>
<td>-</td>
<td>20</td>
</tr>
<tr>
<td>Priority Threshold:</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td>High Pri Service Ratio:</td>
<td>-</td>
<td>1023-to-1</td>
</tr>
<tr>
<td>High Overflow Drops:</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Overflow Drops:</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>High Stale Drops:</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>Stale Drops:</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>

**Systems**  
5 Console

Overview

This chapter describes:

- set console baud
- set console databits
- set console flowcontrol
- set console initcmd
- set console parity
- set console stopbits
- set console transfer ppp
- set console type
- show console
set console baud

Command Mode  Global Configuration.

Description  Sets console port baud rate. The default value is 9600.

Syntax  set console baud \{300| 1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200\}

Sample Output  The following example sets the console baud rate to 19200.

```
(configure)# set console baud 19200
```

set console databits

Command Mode  
Global Configuration.

Description  
Sets the console serial port’s databit width. The default value is 8.

* Note: This command is not applicable when the console serial port is configured in PPP mode. The input will not be accepted or stored when the console serial port is configured in PPP mode.

However, if the console serial port is configured as TTY mode and the databits width is configured, the console serial port can be changed to PPP mode and the databit width is saved until TTY mode is restored.

Syntax  
set console databits {7 | 8}

Table 5-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{7</td>
<td>8}</td>
</tr>
</tbody>
</table>

Sample Output  
This example sets the databit width for the console serial port to 7.

(configure)# set console databits 7

Systems  
set console flowcontrol

**Command Mode**
Global Configuration.

**Description**
Sets the flow control type for the serial console port. The default for both TTY and PPP is xon/xoff.

**Syntax**
```
set console flowcontrol {none | xon/xoff}
```

**Table 5-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{none</td>
<td>xon/xoff}</td>
</tr>
</tbody>
</table>

**Sample Output**
This example sets the console flow control to none.

```
(configure) # set console flowcontrol none
```

**Systems**
set console initcmd

Command Mode  Global Configuration.

Description  Sets the modem initialization string for console serial port modem control software. The default Modem Configuration String is AT&D0S0=1.

* Note: This command is not applicable when the console serial port is configured in TTY mode. The input will not be accepted or stored when the serial port is configured in TTY mode.

The init command string is used to configure the attached external modem so that dial-in sessions will be properly accepted by the modem and the connection successfully completed between the switch and the remote system. The set console initcmd is only accepted when the console serial port is configured as PPP mode. Please read your modem’s reference literature to find the correct AT parameters.

There are few configurations and Avaya recommended modems that do not require a modem initialization string.

Syntax  set console initcmd [init_cmd_string]

Table 5-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[init_cmd_string]</td>
<td>An optional parameter, however, when the parameter is missing, it means that the modem initialization string is &lt;null&gt;.</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the console initialization command with an initialization string of AT&D080=1

```
(configure)# set console initcmd AT&D0S0=1
```

set console parity

**Command Mode**
Global Configuration.

**Description**
* Note: Sets the parity for the console serial port. The default setting is none.

* Note: The concept of parity is not applicable to the console serial port when it is configured in PPP mode. When the console serial port is configured in PPP mode, the parity value cannot be accepted or stored. However, to save a parity value, the console serial port mode can be changed to TTY mode, the parity value set, and the console serial port mode returned to PPP mode. The parity value is saved until the console serial port is reconfigured as TTY mode.

**Syntax**
set console parity {none | even | odd}

**Sample Output**
The following example sets the console parity to even.

```
(configure) # set console parity even
```

**Systems**
**set console stopbits**

**Command Mode**
Global Configuration.

**Description**
Sets the serial console port stopbits to 1 or 2 bits wide. The default setting is 1.

Stopbits is not compatible with the serial console port configured in PPP mode. The stopbits parameter cannot be accepted or saved when the serial console port is configured as PPP mode.

However, to configure the serial console port stopbits parameter, the serial console port can be configured as TTY mode and the stopbits parameter set. The serial console port can then be reconfigured as PPP mode. The stopbits parameter is saved until the console serial port is reconfigured as TTY mode.

**Syntax**
set console stopbits {1 | 2}

**Table 5-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{1</td>
<td>2}</td>
</tr>
</tbody>
</table>

**Sample Output**
This example sets the serial console port stopbits to 2 bits wide

```
(configure)# set console stopbits 2
```

**Systems**
set console transfer ppp

**Command Mode**
Global Configuration.

**Description**
Transfers control of the serial console port and the CLI session to the PPP protocol layer.

This command is accepted only when the console serial port is configured in PPP mode.

When accepted, this command immediately terminates the current CLI session, logs the user out, and switches the I/O on the serial console port from the CLI processing software to the PPP layer. The remote host also needs to simultaneously change its I/O to use PPP software. This command is NOT stored (no back-end), and is only for use when the user has successfully dialed-into the switch. This command can only be accepted when the Console Serial Port is configured in PPP mode.

The command cannot be accepted from a telnet session, it can be accepted only over directly connected serial sessions, and most preferably from a post-dial modem terminal session on the remote host.

**Syntax**
set console transfer ppp

**Sample Output**
The following example sets the console transfer ppp.

(configure) # set console transfer ppp

**Systems**
**set console type**

**Command Mode**
Global Configuration.

**Description**
Sets the console type to the indicated value - either tty or ppp. The default is tty.

**Syntax**
```
set console type {tty | ppp}
```

**Table 5-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{tty</td>
<td>ppp}</td>
</tr>
<tr>
<td></td>
<td>• tty - Sets the serial console port mode to use straight ascii interface, in other words, “dumb terminal.”</td>
</tr>
<tr>
<td></td>
<td>• ppp - Sets the serial console port mode, upon the conclusion of the current TTY:CLI session, to interact with an external modem, and to permit the use of a PPP connection and PPP packets contained in Async-PPP frames.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the console type to tty.

```
(configure)# set console type ppp
```

**Systems**
show console

**Command Mode**  
User.

**Description**  
Displays the serial console port configuration.

**Syntax**  
show console

**Sample Output**  
The following example displays the serial port configuration information.

```plaintext
> show console
  Type: TTY
  Baudrate: 9600 bps
  Flow control: XON/XOFF
  Data bits: 8
  Parity: None
  Stop bits: 1
```

**Systems**  
6 DNS

Overview

This chapter describes the following commands:

- ip domain-lookup
- ip name-server
- ip domain-list
- ip domain-name
- show host
**ip domain-lookup**

**Command Mode**  
Global Configuration.

**Description**  
Enables DNS client. The no form of this command disables DNS client.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip domain-lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip domain-lookup</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example enables DNS.

```
(configure)# ip domain-lookup
```

**Systems**  
ip name-server

Command Mode  Global Configuration.

Description  Adds a DNS server address. The no form of this command removes the DNS server address.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip name-server &lt;ip address&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip name-server &lt;ip address&gt;</td>
</tr>
</tbody>
</table>

Sample Output  The following example adds the DNS server with an IP address of 210.120.87.90.

    (configure)# ip name-server 210.120.87.90

**ip domain-list**

**Command Mode**
Global Configuration.

**Description**
Adds a domain name to the domain name list. The **no** form of this command removes the domain name.

**Syntax**

<table>
<thead>
<tr>
<th><strong>To Enable:</strong></th>
<th>ip domain-list &lt;name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Disable:</strong></td>
<td>no ip domain-list &lt;name&gt;</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example adds the name “avaya.com” to the DNS name list.

(configure) # ip domain-list avaya.com

**Systems**
**ip domain-name**

**Command Mode**
Global Configuration.

**Description**
Adds a domain name to the domain name list. The no form of this command removes the domain name.

**Syntax**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Enable:</strong></td>
<td>ip domain-name &lt;domain-name&gt;</td>
</tr>
<tr>
<td><strong>To Disable:</strong></td>
<td>no ip domain-name &lt;domain-name&gt;</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example adds the name “avaya.com” to the DNS name list.

```
(configure)# ip domain-name avaya.com
```

**Systems**
show host

Command Mode      Global Configuration.

Description       Displays the DNS domain configuration.

Syntax            show host

Sample Output      The following example displays the DNS configuration:

                  (configure) # show host

Overview

This chapter describes the following commands:

- `ip dvmrp`
- `ip dvmrp interface type`
- `ip dvmrp interface-metric`
- `ip dvmrp min-route-flash-update`
- `ip dvmrp neighbor-probe-interval`
- `ip dvmrp neighbor-timeout`
- `ip dvmrp prune-message-lifetime`
- `ip dvmrp remote-tunnel-address`
- `ip dvmrp route-limit`
- `ip dvmrp stats-reset`
- `ip dvmrp timers basic`
- `ip multicast prune-source`
- `ip multicast ttl-threshold`
- `router dvmrp`
- `show ip dvmrp`
- `show ip dvmrp designated forwarders`
- `show ip dvmrp downstream dependent routers`
- `show ip dvmrp forwarding cache`
- `show ip dvmrp interface`
- `show ip dvmrp interface neighbors`
- `show ip dvmrp routes`
ip dvmrp

Command Mode  Interface Configuration.

Description  Enables and configure DVMRP services on an interface. The no form of this command disables DVMRP services on an interface.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip dvmrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip dvmrp</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables dvmrp on an interface.

(config-if:boston)# ip dvmrp

ip dvmrp interface-metric

Command Mode
Interface Configuration.

Description
Configures the DVMRP interface metric. The no form of this command restores the default, which is 1.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip dvmrp interface-metric &lt;intf-metric&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip dvmrp interface-metric</td>
</tr>
</tbody>
</table>

Table 7-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;intf-metric&gt;</td>
<td>DVMRP interface metric or hop count. The valid range is 1 to 31 hops. The default setting is 1.</td>
</tr>
</tbody>
</table>

Sample Output
The following example configures the interface labeled “boston” with a DVMRP interface metric of 2.

(config-if:boston)# ip dvmrp interface-metric 2

Systems
**Command Mode**

Interface Configuration.

**Description**

Configures the DVMRP interface type. The no form of this command restores the interface to the default interface type, which is broadcast.

**Syntax**

| To Configure: | ip dvmrp interface type {broadcast | nonEncapsulatedTunnel | IPIPTunnel} |
|---------------|---------------------------------------------------|
| To Restore Default: | [no] ip dvmrp interface type |

**Table 7-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface type</td>
<td>DVMRP interface type. The case-sensitive keywords are broadcast (default), nonEncapsulatedTunnel, and IPIPTunnel.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example configures interface “boston” as a DVMRP IPIPTunnel.

```
(config-if:boston)# ip dvmrp interface type IPIPTunnel
```

**Systems**

ip dvmrp min-route-flash-update

Command Mode
DVMRP Router Configuration.

Description
Sets the DVMRP minimum route flash update period. Use the no form of this command to return to the default value of 5.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip dvmrp min-route-flash-update &lt;min-update-value&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip dvmrp min-route-flash-update</td>
</tr>
</tbody>
</table>

Table 7-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;min-update-value&gt;</td>
<td>The DVMRP minimum route flash update period, measured in seconds.</td>
</tr>
<tr>
<td></td>
<td>The valid range is 5 to 20 seconds. The default setting is 5 seconds</td>
</tr>
</tbody>
</table>

Sample Output
The following example configures the ip dvmrp minimum route flash update period for ten seconds.

```
(configure router:dvmrp) # ip dvmrp min-route-flash-update 10
```

Systems
**ip dvmrp neighbor-probe-interval**

**Command Mode**: DVMRP Router Configuration.

**Description**: Sets the DVMRP neighbor probe interval. Use the no form of this command to return to the default value of 10 seconds.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip dvmrp neighbor-probe-interval &lt;neighbor-probe&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip dvmrp neighbor-probe-interval</td>
</tr>
</tbody>
</table>

**Table 7-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;neighbor-probe&gt;</td>
<td>The DVMRP neighbor probe interval, which is measured in seconds. The valid range is 5-45 seconds. The default setting is 10 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**: The following example configures the IP DVMRP neighbor probe interval for eleven seconds.

```
(configure router:dvmrp)# ip dvmrp neighbor-probe-interval 11
```

ip dvmrp neighbor-timeout

**Command Mode**
DVMRP Router Configuration.

**Description**
Sets the DVMRP neighbor timeout interval. Use the no form of this command to return to the default value of 35 seconds.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip dvmrp neighbor-timeout <em>&lt;neighbor-timeout&gt;</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip dvmrp neighbor-timeout</td>
</tr>
</tbody>
</table>

**Table 7-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>&lt;neighbor-timeout&gt;</em></td>
<td>The DVMRP neighbor timeout interval, which is measured in seconds.</td>
</tr>
<tr>
<td></td>
<td>The valid range is 10 to 50 seconds. The default setting is 35 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example configures the IP DVMRP neighbor timeout interval for thirty-six seconds.

```
(configure router:dvmrp)# ip dvmrp neighbor-timeout 36
```

**Systems**
**ip dvmrp prune-message-lifetime**

**Command Mode**
DVMRP Router Configuration.

**Description**
Sets the DVMRP prune message lifetime. Use the no form of this command to return to the default value of 7200 seconds.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip dvmrp prune-message-lifetime <code>&lt;prune-lifetime&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip dvmrp prune-message-lifetime</td>
</tr>
</tbody>
</table>

**Table 7-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;prune-lifetime&gt;</code></td>
<td>The DVMRP upstream prune message lifetime. The message lifetime is measured in seconds. The valid range is 100-7,200 seconds. The default setting is 7,200 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example configures the IP DVMRP prune message lifetime for fifteen hundred seconds.

```
(configure router:dvmrp)# ip dvmrp prune-message-lifetime 1500
```

**Systems**
ip dvmrp remote-tunnel-address

Command Mode
Interface Configuration.

Description
Configures the DVMRP remote-tunnel-address on an interface. The no form of this command restores the default, which is: no defined address.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip dvmrp remote-tunnel-address &lt;ip-addr&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip dvmrp remote-tunnel-address</td>
</tr>
</tbody>
</table>

Table 7-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>Unicast Network IP address of the DVMRP capable router designated to be DVMRP tunnel end point.</td>
</tr>
</tbody>
</table>

Sample Output
The following example configures the DVMRP remote tunnel address on interface 199.162.99.61.

```
(configure if:1)# ip dvmrp remote-tunnel-address 199.162.99.61
```

Systems
Chapter 7

ip dvmrp route-limit

Command Mode
DVMRP Router Configuration.

Description
Sets the maximum routes allowed in DVMRP. Use the no form of this command to return to the default value of 7000 routes.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip dvmrp route-limit &lt;route-limit&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip dvmrp route-limit</td>
</tr>
</tbody>
</table>

Table 7-8. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;route-limit&gt;</td>
<td>The maximum number of routes allowed. The valid range is 10 to 20,000. The default setting is 7,000</td>
</tr>
</tbody>
</table>

Sample Output
The following example configures the IP DVMRP route limit to five thousand, five hundred.

(configure router:dvmrp)# ip dvmrp route-limit 5500

Systems
### ip dvmrp stats-reset

<table>
<thead>
<tr>
<th><strong>Command Mode</strong></th>
<th>DVMRP Router Configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Resets the DVMRP global statistics.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td>ip dvmrp stats-reset</td>
</tr>
<tr>
<td><strong>Sample Output</strong></td>
<td>The following example shows the command for IP DVMRP stats-reset.</td>
</tr>
<tr>
<td></td>
<td><code>(configure router:dvmrp)# ip dvmrp stats-reset</code></td>
</tr>
</tbody>
</table>
ip dvmrp timers basic

**Command Mode**

DVMRP Router Configuration.

**Description**

Adjusts the DVMRP network timers. Use the no form of this command to return to the default values.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip dvmrp timers basic (&lt;rte-update&gt;) (&lt;rte-expire&gt;) (&lt;rte-holddown&gt;)</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip dvmrp timers basic</td>
</tr>
</tbody>
</table>

**Table 7-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>(&lt;rte-update&gt;)</td>
<td>Configures the DVMRP route reporting interval. The range of frequencies at which updates are sent is 30 to 90 seconds. The default setting is 60 seconds.</td>
</tr>
<tr>
<td>(&lt;rte-expire&gt;)</td>
<td>Interval of time, in seconds, after which a DVMRP route expires. The valid range is 70 to 190 seconds. The default value is 140 seconds.</td>
</tr>
<tr>
<td>(&lt;rte-holddown&gt;)</td>
<td>The amount of time, in seconds, that must pass before the route is removed from the routing table. The valid range is 120-380 seconds. The default setting is 120 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example configures the IP DVMRP timers basic with route update time of 35 seconds, a route expiration time of 75 seconds and route holddown time of 145 seconds.

```
(configure router:dvmrp) # ip dvmrp timers basic 35 75 145
```

**Systems**

ip multicast prune-source

Command Mode
Interface Configuration.

Description
Configures the host address used in DVMRP prune packets forwarded on this interface. The no form of this command restores the default, which is host-addr.

Syntax

| To Configure:           | ip multicast prune-source {host-addr | network-addr} |
|-------------------------|-----------------|
| To Restore Default:    | [no] ip multicast prune-source |

Table 7-10. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-addr</td>
<td>The full host address is used in the prune packet for the source address.</td>
</tr>
<tr>
<td>network-addr</td>
<td>Only the network portion of the address is used in the prune packet.</td>
</tr>
</tbody>
</table>

Sample Output
The following example configures the DVMRP prune packets to the host address for interface 1.

(configure if:1)# ip multicast prune-source host-addr

Systems
**ip multicast ttl-threshold**

**Command Mode**  
Interface Configuration.

**Description**  
Sets the minimum TTL (time-to-live) required for a packet to leave the interface. The no form of this command restores the default (none).

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip multicast ttl-threshold <code>&lt;ttl-thresh&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip multicast ttl-threshold</td>
</tr>
</tbody>
</table>

**Table 7-11. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ttl-thresh&gt;</code></td>
<td>Indicates the time to live threshold: The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• 0- None</td>
</tr>
<tr>
<td></td>
<td>• 127</td>
</tr>
<tr>
<td></td>
<td>• 2-255 - only outbound broadcasts are accepted.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the minimum TTL required for a packet to leave interface 1 to 127.

```
(configure if:1)# ip multicast ttl-threshold 127
```

**Systems**  
router dvmrp

Command Mode
Global Configuration.

Description
Enables DVMRP routing globally on an interface. The no form of the command disables DVMRP routing. The default state is Enabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>router dvmrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] router dvmrp</td>
</tr>
</tbody>
</table>

Sample Output
The following example enables DVMRP routing.

```
(configure)# router dvmrp
```

Systems
show ip dvmrp

**Command Mode**
User.

**Description**
Displays configuration information about the DVMRP protocol.

**Syntax**
show ip dvmrp

**Sample Output**
The following example displays the DVMRP global configuration information with some statistics.

```
> show ip dvmrp
DVMRP state is Enabled

  Neighbor probe interval: 10
  Neighbor timeout interval: 35
  Minimum flash update interval: 5
  Maximum number of routes allowed: 7000
  Route report interval: 60
  Route expire period: 140
  Route holddown period: 120
  Prune message lifetime: 7200
  Prune message retransmit interval: 3
  Graft message retransmit interval: 5

Global Statistics
  Probe messages received: 014181
  Probe messages transmitted: 22272
  Report messages received: 2462
  Report messages transmitted: 1412
  Prune messages received: 1
  Prune messages transmitted: 6
  Graft messages received: 2
  Graft messages transmitted: 5
  Graft acknowledge messages received: 3
  Graft acknowledge messages transmitted: 2
  Unknown messages received: 0
  Valid route report messages received: 3
  Total remote and local route entries: 3
  Total triggered route entries: 0
```

**Systems**
show ip dvmrp designated forwarders

Command Mode
User.

Description
Displays all DVMRP designated forwarding routers for the source network address and address mask.

Syntax
show ip dvmrp designated forwarders <ip-addr> <mask>

Table 7-12. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>designated forwarders</td>
<td>Display DVMRP designated forwarder information.</td>
</tr>
<tr>
<td></td>
<td>• &lt;ip-addr&gt; - the source network address.</td>
</tr>
<tr>
<td></td>
<td>• &lt;mask&gt; - the mask for the source network address.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays the DVMRP designated forwarding routers for ip address 20.0.4.0 and mask 255.255.255.0.

> show ip dvmrp designated forwarders 20.0.4.0 255.255.255.0
DVMRP designated forwarders for route entry 20.0.4.0/255.255.255.0
Forwarder interface: vlan9
Forwarder network address: 9.0.0.100
Forwarder cost to source network: 3

Forwarder interface: vlan11
Forwarder network address: 11.0.0.10
Forwarder cost to source network: 2

Forwarder interface: Test70 VLAN: VLAN70
Forwarder network address: 10.4.53.102
Forwarder cost to source network: 1

Forwarder interface: SW Lab VLAN71
Forwarded Network Address: 171.102.0.1
Forwarder cost to source network: 1

Systems
**show ip dvmrp downstream dependent routers**

**Command Mode**  User.

**Description**  Displays all DVMRP downstream dependent neighbor routers for the source network address and address mask.

**Syntax**  
```
show ip dvmrp downstream dependent routers <ip-addr> <mask>
```

**Sample Output**

The following example displays all DVMRP downstream dependent neighbor routers for ip address 20.0.4.0 and mask 255.255.255.0.

```
> show ip dvmrp downstream dependent routers 20.0.4.0 255.255.255.0
DVMRP designated forwarders for route entry 44.0.0.0/255.0.0.0
Neighbor network adders: 9.0.0.10
Found on interface: vlan9
Neighbor supported major/minor version 3/0xFF
Neighbor received probe from this router: Yes
Neighbor supports prune function: Yes
Neighbor supports generation ID function: Yes
Neighbor supports MTRACE requests: No
Neighbor is SNMP manageable: Yes
```


<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>downstream dependent routers</td>
<td>Display DVMRP downstream dependency information.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;ip-addr&gt;</code> - The source network address IP address.</td>
</tr>
<tr>
<td></td>
<td>• <code>&lt;mask&gt;</code> - The mask for the source network address IP subnet.</td>
</tr>
</tbody>
</table>

**Table 7-13. Parameters, Keywords, Arguments**
**show ip dvmrp forwarding cache**

**Command Mode** User.

**Description** Displays the DVMRP Multicast Forwarding Cache.

**Syntax** `show ip dvmrp forwarding cache`

**Sample Output** The following example displays the DVMRP Multicast Forwarding cache.

```
> show ip dvmrp forwarding cache
  DVMRP forwarding cache
  Destination group address: 225.0.0.100
  Source subnetwork: 10.4.32.0
  Source address mask: 255.255.255.0
  Upstream interface: Accounting
  Upstream VLAN: VLAN70
  Upstream neighbor (router) address: 10.4.54.105
  Invalid flows from upstream: 0
  Packets forwarded through cache entry: 1
  Upstream interface is pruned: Yes
  Next pruned downstream interface to timeout: None
  Downstream interface(s): Filtered
    Interface: Video_Feed VLAN: VLAN60
    Interface type: Broadcast
    Interface is pruned: No
    Prune expiration time in (sec):n/a
  Upstream source(s)
    Flow source address: 33.33.33.34
    Payload protocol type: UDP
    Source port number: 3280
    Destination port number: 49153

show ip dvmrp interface

Command Mode  
User.

Description  
Displays the related information about the DVMRP interface.

Syntax  
show ip dvmrp interface

Sample Output  
The following example displays information for an ip DVMRP interface

> show ip dvmrp interface
DVMRP circuit IFIndex 8 on interface vlan40 state is up

  Interface address and mask: 10.0.4.94/255.255.255.0  
  Interface type: Broadcast  
  Prune message flow source address: Use source host address  
  Current neighbors on interface: 0  
  Interface metric: 1  
  Interface scope: 0  
  Invalid protocol message received: 0  
  Invalid route messages received: 0  
  Route messages transmitted: 13320

Systems  
show ip dvmrp interface neighbors

Command Mode: User.

Description: Displays all DVMRP neighbors on all DVMRP configured interfaces.

Syntax: show ip dvmrp interface neighbors

Sample Output: The following example displays all DVMRP neighbors on all of the configure DVMRP interfaces on the switch.

```
> show ip dvmrp interface neighbors
DVMRP neighbor routers on interface vlan9

Neighbor network address: 9.0.0.10
Neighbor supported major/minor version: 3/0x0FF
Neighbor expiration period in (sec): 27
Neighbor received probe from this router: Yes
Neighbor supports prune function: Yes
Neighbor supports generation ID function: No
Neighbor supports MTRACE requests: No
Neighbor is SNMP manageable: Yes

```
**show ip dvmrp routes**

**Command Mode**  
User.

**Description**  
Displays all DVMRP routes.

**Syntax**  
show ip dvmrp routes

**Sample Output**  
The following example displays all DVMRP routes.

```plaintext
> show ip dvmrp routes
DVMRP route table

Source network and mask: 10.0.4.94/255.255.255.0
Reporting router: 10.0.6.96
Reporting router interface: Software_Lab
Reporting router vlan: vlan60
Route metric: 3
Expiration period in (sec): 18
.
.
Source network and mask: 171.102.0.0/255.255.0.0
Local Interface: Hardware_Lab
Local VLAN: VLAN 71
Route metric: 1
```

**Systems**  
8 Hunt Groups

Overview

This chapter describes:

- `set huntgroup`
- `set huntgroup auto-flush`
- `set huntgroup (redistribute)`
- `set huntgroup internal-error-shutdown`
- `show huntgroup`
- `show huntgroup detailed`
- `show huntgroup internal-error-config`
set huntgroup

Command Mode: Global Configuration.

Description: Creates a huntgroup, modifies an existing huntgroup or removes a huntgroup. If no load-sharing value is specified, then a huntgroup is created with load-sharing enabled. Use the `clear huntgroup` form of this command to remove a huntgroup.

Syntax:

| To Configure:          | set huntgroup <huntgroup-name> [load-sharing {enable | disable}] |
|------------------------|-----------------------------------------------------------------|
| To Delete:             | clear huntgroup <huntgroup-name>                                |

Table 8-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;huntgroup-name&gt;</td>
<td>The unique string used to identify a huntgroup. If the name is not unique to the huntgroup, then it is assumed that an existing huntgroup is being modified.</td>
</tr>
</tbody>
</table>
| load-sharing        | The load sharing capability.  
|                     | • {enable | disable} - Enables or disables load sharing. |

Sample Output: The following example creates huntgroup hg1 and disables load-sharing.

```
(configure)# set huntgroup hg1 load-sharing disable
HuntGroup “hg1” created
```

set huntgroup auto-flush

**Command Mode**
Global Configuration.

**Description**
Enables or disables the auto flush feature for the ports participating in a hunt group.

When you enable auto flush for a hunt group, all AFT entries that were learned on the hunt group are marked invalid if the links to all of the hunt group ports fail. Once the AFT entries are marked invalid, they can be learned on a redundant port. When auto flush is enabled, failover to a redundant port occurs much sooner.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set huntgroup auto-flush &lt;huntgroup-name&gt; enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set huntgroup auto-flush &lt;huntgroup-name&gt; disable</td>
</tr>
</tbody>
</table>

**Table 8-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;huntgroup-name&gt;</td>
<td>The huntgroup for which you want to enable or disable auto flush.</td>
</tr>
<tr>
<td>{enable</td>
<td>disable}</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
set huntgroup (redistribute)

**Command Mode**
Global Configuration.

**Description**
Redistributes learned addresses to a huntgroup. The MAC addresses are redistributed among the huntgroup ports.

**Syntax**
```
set huntgroup <huntgroup-name> redistribute
```

**Table 8-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;huntgroup-name&gt;</td>
<td>The unique identifier of a huntgroup.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example redistributes huntgroup 1 (hg1).

```
(configure)# set huntgroup hg1 redistribute
HuntGroup “hg1” successfully redistributed
```

**Systems**
set huntgroup internal-error-shutdown

Command Mode  Global Configuration.

Description  Enables or disables internal-error-shutdown on the huntgroup.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set huntgroup internal-error-shutdown enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set huntgroup internal-error-shutdown disable</td>
</tr>
</tbody>
</table>

Sample Output

The following example enables internal-error-shutdown on a huntgroup.

```
(configure)# set huntgroup internal-error-shutdown enable
```

Systems

show huntgroup

Command Mode  User.

Description  Displays a single huntgroup or, if no huntgroup name is specified, then all of the configured huntgroups display.

Syntax  show huntgroup [<huntgroup-name>]

Table 8-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;huntgroup-name&gt;</td>
<td>The name of the huntgroup to be displayed.</td>
</tr>
</tbody>
</table>

Sample Output  The following example shows detailed huntgroup information.

> show huntgroup 1

<table>
<thead>
<tr>
<th>huntgroup name</th>
<th>HGID</th>
<th>Port</th>
<th>SharingPorts</th>
</tr>
</thead>
<tbody>
<tr>
<td>huntgroup</td>
<td>1</td>
<td>1</td>
<td>Enable 0</td>
</tr>
</tbody>
</table>

show huntgroup detailed

Command Mode User.

Description Displays detailed information about all of the huntgroups configured on your switch.

Syntax show huntgroup detailed

Sample Output

The following example shows detailed huntgroup information.

> show huntgroup detailed

<table>
<thead>
<tr>
<th>huntgroup name</th>
<th>HGID</th>
<th>Port</th>
<th>Sharing Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>huntgroup 1</td>
<td>1</td>
<td>1</td>
<td>Enable 0</td>
</tr>
</tbody>
</table>

show huntgroup internal-error-config

**Command Mode**  
User.

**Description**  
Displays the status of internal-error-detection on the hunt group.

**Syntax**  
show huntgroup internal-error-config

**Sample Output**  
The following example displays the status of internal-error-detection for the huntgroup.

```
(configure)# show huntgroup internal-error-config
HuntGroup internal-error-detection enabled
```

**Systems**  
9  IGMP

Overview

This chapter describes the following commands:

- ip igmp
- ip igmp max-groups
- ip igmp process-leaves
- ip igmp querier
- ip igmp querier-timeout
- ip igmp query-interval
- ip igmp query-max-response-time
- ip igmp query-timeout
- ip igmp robustness
- ip igmp version
- ip mtrace
- mtrace
- router igmp
- show ip igmp groups
- show ip igmp interface
- show ip igmp interface
ip igmp

**Command Mode**  
Interface Configuration.

**Description**  
Enables the Internet Group Management Protocol (IGMP) on an interface. The no form of this command disables IGMP on an interface.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip igmp</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip igmp</td>
</tr>
</tbody>
</table>

**Syntax**

The following example enables igmp on the interface labeled “boston”

```
(config-if:boston)# ip igmp
```

**Systems**

ip igmp max-groups

Command Mode Interface Configuration.

Description Sets the maximum number of IGMP groups on an interface. The no form of this command restores the default value, which is 32 groups.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip igmp max-groups &lt;number&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip igmp max-groups</td>
</tr>
</tbody>
</table>

Table 9-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;number&gt;</td>
<td>Maximum number IGMP groups on the interface. The valid range is 1 to 7000. The default setting is 32.</td>
</tr>
</tbody>
</table>

Sample Output The following example sets the maximum number of IGMP groups on interface labelled “Boston” to 50.

(config-if:boston)# ip igmp max-groups 50

**ip igmp process-leaves**

**Command Mode**
Interface Configuration.

**Description**
Enables the processing of leave requests on an interface. The no form of this command disables the processing of leave requests on an interface and returns it to the default state: enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip igmp process-leaves 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>ip igmp process-leaves 0</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables the processing of leave requests on interface labelled boston.

```
(config-if:boston)# ip igmp process-leaves 1
```

**Systems**
**ip igmp querier**

**Command Mode**  Interface Configuration.

**Description**  Enables IGMP querier on an interface on a router.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip igmp querier 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>ip igmp querier 0</td>
</tr>
</tbody>
</table>

**Sample Output**  The following example enables IGMP querier on interface labeled “boston”.

(config-if:boston)# ip igmp querier 1

### ip igmp querier-timeout

**Command Mode**  
Interface Configuration.

**Description**  
Sets the time that needs to elapse from the time the last query was heard before this router takes over as a designated querier for the interface. The no form of this command restores the default value of 255 seconds.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip igmp querier-timeout &lt;nbr-qry&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip igmp querier-timeout</td>
</tr>
</tbody>
</table>

**Table 9-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;nbr-qry&gt;</td>
<td>The neighbor group querier timeout in seconds. The range is 30-600 seconds. The default setting is 255 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example configures the time out period before the router takes over as the querier on an interface labeled “boston” to 250 seconds.

```
(config-if:boston)# ip igmp querier-timeout 250
```

**Systems**

ip igmp query-interval

Command Mode
Interface Configuration.

Description
Configures the frequency at which the router sends IGMP host-query messages. The no form of this command restores the default value of 125 seconds.

Syntax

<table>
<thead>
<tr>
<th>To Configure</th>
<th>ip igmp query-interval &lt;req-intvl&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip igmp query-interval</td>
</tr>
</tbody>
</table>

Table 9-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;req-intvl&gt;</td>
<td>The number of seconds between host-query messages. The valid range is 1 to 65,535 seconds. The default setting is 125 seconds.</td>
</tr>
</tbody>
</table>

Sample Output
The following example configures the frequency at which the router sends IGMP host query messages on interface labelled “boston” to 125 seconds.

(config-if:boston)# ip igmp query-interval 125

Systems
**ip igmp query-max-response-time**

**Command Mode**  
Interface Configuration.

**Description**  
Configures the maximum response time advertised in IGMP queries. The no form of this command restores the default value of 10 seconds.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip igmp query-max-response-time <code>&lt;max-rsp-intvl&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip igmp query-max-response-time</td>
</tr>
</tbody>
</table>

**Table 9-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;max-rsp-intvl&gt;</code></td>
<td>The maximum response time advertised in IGMP queries. The valid range is 1-25 seconds. The default setting is 10 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example configures the maximum response time advertised in IGMP queries on interface labeled “boston” to 25 seconds.

```
(config-if:boston)# ip igmp query-max-response-time 25
```

**Systems**  
**ip igmp query-timeout**

**Command Mode**  
Interface Configuration.

**Description**  
Sets the time that needs to elapse from the time the last query was heard before this router takes over as a designated querier for the interface. The no form of this command restores the default value of 255 seconds.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip igmp query-timeout &lt;nbr-qry&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip igmp query-timeout</td>
</tr>
</tbody>
</table>

**Table 9-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;nbr-qry&gt;</td>
<td>The neighbor group querier timeout in seconds. The range is 30-600 seconds. The default setting is 255 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example configures the time out period before the router takes over as the querier on an interface labeled “boston” to 250 seconds.

```
(config-if:boston)# ip igmp query-timeout 250
```

**Systems**  
ip igmp robustness

Command Mode  Interface Configuration.

Description  Configures the IGMP robustness variable. Use the no form of this command to restore the default value of 2.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip igmp robustness &lt;robustness&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip igmp robustness</td>
</tr>
</tbody>
</table>

Table 9-6. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;robustness&gt;</td>
<td>IGMP robustness variable. The valid range is 1 to 65,535. The default setting is 2.</td>
</tr>
</tbody>
</table>

Sample Output  The following example configures the IGMP robustness variable on an interface labeled “boston” to 100 seconds.

(config-if:boston)# ip igmp robustness 100

ip igmp version

Command Mode Interface Configuration.

Description Configures which IGMP version the router will use. Use the no form of this command to restore the default value of 2.

Syntax

| To Configure: | ip igmp version {2 | 1} |
|---------------|-------------------------|
| To Restore Default: | [no] ip igmp version |

Sample Output The following example configures the router on an interface labeled “boston” to use IGMP version 1.

(config-if:boston)# ip igmp version 1

**ip mtrace**

**Command Mode**  
User.

**Description**  
Globally configures MTrace capability on this router. The **no** form of this command disables MTrace capability.

**Syntax**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Enable:</strong></td>
<td>ip mtrace</td>
</tr>
<tr>
<td><strong>To Disable:</strong></td>
<td>no ip mtrace</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example configures IP mtrace capability on the router.

```plaintext
> ip mtrace
```

**Systems**  
mtrace

Command Mode
Privileged.

Description
Traces the path from a source to a destination branch for a multicast distribution tree. The trace follows the multicast path from the destination to the source by passing an mtrace request packet to each hop. The responses are unicast to the querying router by the first hop router to the source. The mtrace command is helpful in isolating multicast routing failures.

Syntax
mtrace <source> [<destination>] [<group>]

Table 9-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;source&gt;</td>
<td>The IP address of the Multicast Capable source. This is a unicast address that represents the beginning of the path to be traced.</td>
</tr>
<tr>
<td>&lt;destination&gt;</td>
<td>The IP address of the unicast destination. If omitted, the trace starts from the system at which the command is typed.</td>
</tr>
<tr>
<td>&lt;group&gt;</td>
<td>The Multicast Address of the group address to be traced. The default address is: 224.2.0.1. (The group used for MBONE audio.)</td>
</tr>
</tbody>
</table>

Sample Output
The following example traces the path from a source (10.0.2.129) to a destination (10.0.4.77) branch for a multicast destination tree (255.0.1.1).

```
# mtrace 10.0.2.129 10.0.4.177 255.0.1.1
        OutIntf   InIntf   Port  Fwd     TTL
  -1  10.0.6.96, 10.0.5.96 DVMRP    thresh^32 0 ms
  -2  10.0.5.95, 10.0.1.95 DVMRP    thresh^32 1391000 ms
  -3  10.0.2.63, 10.0.1.63 DVMRP    thresh^32 2054500 ms
Round trip time 0 ms
```

Systems
**router igmp**

**Command Mode**
Global Configuration.

**Description**
Globally enables or disables IGMP. The no form of the command disables IGMP. The default state is: Enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>router igmp</th>
</tr>
</thead>
</table>

| To Disable: | [no] router igmp |

**Sample Output**
The following example globally disables IGMP on the switch.

```
(configure)# no router igmp
```

**Systems**
show ip igmp groups

Command Mode User.

Description Displays multicast groups, learned but this router via IGMP.

Syntax show ip igmp groups

Sample Output The following example displays multicast groups learned by this router via IGMP.

> show ip igmp groups
GROUP<s> for Accounting.State is up.
GROUP<s> for Software Lab.State is up
GROUP<s> for Video.Feed.State is up.
  Group Address is 239.255.0.1
  Group Reporter Address is 20.0.4.41
  Entry Expiration Period in (sec) is 193
  Group Created on 02-May-21 17:38:59

show ip igmp interface

Command Mode
User.

Description
Displays IGMP interface configuration.

Syntax
show ip igmp interface

Sample Output
The following example displays IP IGMP interface information on the switch.

> show ip igmp interface
  30net is down
  Internet address is 30.30.1.0 Subnet
  Mask is 255.255.0.0
  IGMP is enabled on interface?: TRUE
  IP multicast forwarding enabled on interface: FALSE
  IGMP version running is v2
  Maximum number of groups allowed on interface is 32
  Group queries are Enabled? FALSE?
  Processing of Leave Requests is Enabled? TRUE?
  Interval between General Queries sent is 125
  Maximum Response Time inserted into General Queries is 10
  Neighbor Group querier timeout in seconds is 255
  Robustness variable is 2
  Current state of IGMP on this interface is DOWN

Systems
show ip igmp statistics

Command Mode  User.
Description  Displays IGMP statistics for all interfaces.
Syntax  show ip igmp statistics
Sample Output  The following example displays IGMP statistics for all of the interfaces configured on the switch.

  > show ip igmp statistics
      intf4 is up
      Internet address is 10.0.4.94, subnet mask is 255.255.255.0
      Next Query Request in seconds 113
      Neighbor Querier Timeout in seconds 0
      Number of Group Join Requests Received on this interface 110
      Number of Group Leave Request Received on this interface 0
      Number of Group Reports Received on this interface 4711
      Number of Unknown Messages Received on this interface 0
      Number of Current Groups on this interface 7

10 Intelligent Multicast

Overview

This chapter describes the following commands:

- clear cgmp statistics
- clear igmp-snooping statistics
- clear intelligent-multicast client-port
- clear intelligent-multicast router-port
- clear intelligent-multicast session
- clear intelligent-multicast static-client-port
- clear intelligent-multicast static-session
- clear lgmp client statistics
- clear lgmp server statistics
- set cgmp
- set igmp-snooping
- set intelligent-multicast
- set intelligent-multicast client-leave-processing
- set intelligent-multicast client-port-pruning
- set intelligent-multicast client-port-pruning time
- set intelligent-multicast router-port
- set intelligent-multicast router-port-pruning time
- set intelligent-multicast session-pruning
- set intelligent-multicast session-pruning time
- set intelligent-multicast static-client-port
- set intelligent-multicast static-session
- set lgmp client
■ set lgmp server
■ set lgmp server priority
■ set lgmp server proxy
■ set lgmp server router-report-time
■ set lgmp server robust-variable
■ show cgmp statistics
■ show igmp-snooping statistics
■ show intelligent-multicast client-port
■ show intelligent-multicast configuration
■ show intelligent-multicast router-port
■ show intelligent-multicast session
■ show intelligent-multicast static-client
■ show intelligent-multicast static-session
■ show lgmp client
■ show lgmp server
# clear cgmp statistics

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Global Configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Clears CGMP snooping statistics.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td>clear cgmp statistics</td>
</tr>
<tr>
<td><strong>Sample Output</strong></td>
<td>The following example clears cgmp snooping statistics.</td>
</tr>
<tr>
<td><strong>clear igmp-snooping statistics</strong></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Command Mode</strong></td>
<td>Global Configuration.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Clears IGMP snooping statistics.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td>clear igmp-snooping statistics</td>
</tr>
<tr>
<td><strong>Sample Output</strong></td>
<td>The following example clears igmp snooping statistics.</td>
</tr>
<tr>
<td></td>
<td>(configure) # clear igmp snooping statistics</td>
</tr>
</tbody>
</table>
clear intelligent-multicast client-port

**Command Mode**
Global Configuration.

**Description**
Removes the specified learned client ports from an Intelligent Multicast session.

**Syntax**
clear intelligent-multicast client-port <session-id> port <port>

**Table 10-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;session-id&gt;</td>
<td>The number assigned to the Intelligent Multicast Session at creation. This number can be found using the show intelligent-multicast session command.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>The switch port assigned to the Intelligent Multicast session.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example removes learned client ports from Intelligent Multicast session 3.

```
(configure)# clear intelligent-multicast client-port 3 port 4/2
```

**Systems**
clear intelligent-multicast router-port

**Command Mode**
Global Configuration.

**Description**
Removes manually or dynamically added router ports.

*Note:* You can remove only one router port at a time. If a router port is configured with `vlan all` then you must clear it with `vlan all`.

**Syntax**
clear intelligent-multicast router-port vlan {all | <vlan-id> | name <vlan-name>} port <mod-port-spec>

**Table 10-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>• all - All VLANs</td>
</tr>
<tr>
<td></td>
<td>• vlan-id - The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td></td>
<td>• name - The VLAN name.</td>
</tr>
<tr>
<td>&lt;mod-port-spec&gt;</td>
<td>Switch port on a module.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example removes router ports for Intelligent Multicasting on all VLANs bound to port 3/4

```
(configure)# clear intelligent-multicast router-port vlan all port 3/4
Multicast Router Port successfully removed
```

**Systems**
clear intelligent-multicast session

Command Mode  Global Configuration.

Description  Removes the specified learned session from Intelligent Multicast.

* Note: You cannot use this command to remove static multicast sessions. This command removes dynamically learned multicast sessions only.

Syntax  

clear intelligent-multicast session <session-id>

Table 10-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;session-id&gt;</td>
<td>A number assigned to the Multicast Session when it is created. This number can be found in the show intelligent-multicast session display.</td>
</tr>
</tbody>
</table>

Sample Output  The following example clears an Intelligent Multicast session.

(configure)# clear intelligent-multicast session 3

clear intelligent-multicast static-client-port

**Command Mode**

Global Configuration.

**Description**

Removes the specified manually added client port from an Intelligent Multicast session.

**Syntax**

```
clear intelligent-multicast static-client-port { <group-address> | mac-address <mac-address> } vlan { all | <vlan-id> | name <vlan-name> } port <mod-port-spec>
```

**Sample Output**

The following example clears a static client port from an Intelligent Multicast session.

```
(configure)# clear intelligent-multicast static-client-port 225.1.1.2
vlan all port 3/2
Multicast Client successfully destroyed
```

**Systems**


<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;group-address&gt;</td>
<td>The IP address of the multicast group for which the session was created.</td>
</tr>
<tr>
<td>&lt;mac-address&gt;</td>
<td>The MAC address associated with the Intelligent Multicast session.</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td></td>
<td>• all - All VLANs</td>
</tr>
<tr>
<td></td>
<td>• vlan-id - The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td></td>
<td>• name - The VLAN name.</td>
</tr>
<tr>
<td>&lt;mod-port-spec&gt;</td>
<td>Switch port on a module.</td>
</tr>
</tbody>
</table>
clear intelligent-multicast static-session

Command Mode  Global Configuration.

Description  Removes manually created Intelligent Multicast sessions.

Syntax  

```
clear intelligent-multicast static-session { <group-address> | mac-address <mac-address> } vlan { all | <vlan-id> | name <vlan-name> }
```

Table 10-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;group-address&gt;</td>
<td>The IP address of the multicast group for which the session was created.</td>
</tr>
<tr>
<td>&lt;mac-address&gt;</td>
<td>The MAC address associated with the Intelligent Multicast session.</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td></td>
<td>• all - All VLANs</td>
</tr>
<tr>
<td></td>
<td>• vlan-id - The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td></td>
<td>• name - The VLAN name.</td>
</tr>
</tbody>
</table>

Sample Output  The following example clears an intelligent-multicast static session.

```
(configure)# clear intelligent-multicast static-session 225.1.1.2 vlan all
Multicast Session successfully destroyed
```

clear lgmp client statistics

**Command Mode**
Global Configuration.

**Description**
Clears LGMP client statistics. If you omit the parameters, this command will clear the global counters representing all LGMP clients.

**Syntax**
clear lgmp client statistics [vlan {all | <vlan-id> | name <vlan-name> }]

**Table 10-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td></td>
<td>• all - All VLANs</td>
</tr>
<tr>
<td></td>
<td>• vlan-id - The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td></td>
<td>• name - The VLAN name.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example clears all lgmp client global statistics.

```
(configure)# clear lgmp client statistics
Global statistics cleared
```

**Systems**
clear lgmp server statistics

Command Mode Global Configuration.

Description Clears the LGMP server global or per VLAN statistics. Excluding parameters clears the global counters that represent all LGMP servers.

Syntax clear lgmp server statistics [vlan {all | <vlan-id> | name <vlan-name> }]

Sample Output

The following example clears all lgmp server statistics.

(configure)# clear lgmp server statistics
Global statistics cleared

set cgmp

Command Mode
Global Configuration.

Description
Enables or disables CGMP snooping functionality. CGMP snooping is disabled by default.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set cgmp enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set cgmp disable</td>
</tr>
</tbody>
</table>

Sample Output
The following example enables cgmp.

(configure)# set cgmp enable

Systems
set igmp-snooping

Command Mode  Global Configuration.

Description  Enables or disables IGMP snooping. The default state of IGMP snooping is disabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set igmp-snooping enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set igmp-snooping disable</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables IGMP snooping.

(configure) # set igmp-snooping enable

set intelligent-multicast

Command Mode  Global Configuration.

Description  Enables or disables Intelligent Multicasting. The default state is enabled.

Syntax

<table>
<thead>
<tr>
<th>Mode</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Enable</td>
<td>set intelligent-multicast enable</td>
</tr>
<tr>
<td>To Disable</td>
<td>set intelligent-multicast disable</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables Intelligent Multicasting.

(configure)# set intelligent-multicast enable

set intelligent-multicast client-leave-processing

Command Mode  Global Configuration.

Description  Configures processing of client port leave messages. The default state of this command is disabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set intelligent-multicast client-leave-processing enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set intelligent-multicast client-leave-processing disable</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables the processing of intelligent-multicast client-leave-processing messages.

```
(configure)# set intelligent-multicast client-leave-processing enable
```

set intelligent-multicast client-port-pruning

**Command Mode**
Global Configuration.

**Description**
Enables or disables automatic client port pruning. The default state of this command is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set intelligent-multicast client-port-pruning enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set intelligent-multicast client-port-pruning disable</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables automatic client port pruning.

```
(configure)# set intelligent-multicast client-port-pruning enable
Client Port Pruning State successfully set to enable
```

**Systems**
set intelligent-multicast client-port-pruning time

**Command Mode**
Global Configuration.

**Description**
Sets the time interval after which a client port will be removed from a session if no IGMP reports have been heard.

The valid range is from 1 minute to 1440 minutes (24 hours). Default time is 60 minutes.

**Syntax**
set intelligent-multicast client-port-pruning time {<minutes>}

**Table 10-8. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;minutes&gt;</td>
<td>The number of minutes that a dynamic Intelligent Multicast client port must be inactive before it is removed from an Intelligent Multicast session.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the intelligent-multicast port pruning time to 45 minutes.

```
(configure)# set intelligent-multicast client-port-pruning time 45
Client Port Pruning Time successfully set to 45 minutes
```

**Systems**
set intelligent-multicast router-port

**Command Mode**  
Global Configuration.

**Description**  
Configures router ports on a selected VLAN or all VLANs. The default state is disabled.

**Syntax**  
set intelligent-multicast router-port vlan {all | <vlan-id> | name <vlan-name>} port <mod-port-spec>

**Table 10-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td></td>
<td>• all - All VLANS.</td>
</tr>
<tr>
<td></td>
<td>• vlan-id - The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td></td>
<td>• name - The VLAN name.</td>
</tr>
<tr>
<td>port</td>
<td>Switch port on a module.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example adds a multicast router port.

```
(configure) # set intelligent-multicast router-port vlan all port 3/4
Multicast Router Port successfully added
```

**Systems**  
set intelligent-multicast router-port-pruning

**Command Mode**  
Global Configuration.

**Description**  
Enables or disables automatic router port pruning. The default state is enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set intelligent-multicast router-port-pruning enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set intelligent-multicast router-port-pruning disable</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example disables router port pruning.

```
(configure)# set intelligent-multicast router-port-pruning disable
```

**Systems**  
set intelligent-multicast router-port-pruning time

Command Mode  Global Configuration.

Description  Sets the time interval after which quiet router ports will be removed.

Syntax  set intelligent-multicast router-port-pruning time <seconds>

Table 10-10. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;seconds&gt;</td>
<td>The number of seconds that a dynamic Intelligent Multicast Router Port must be inactive before it is pruned by the Intelligent Multicast functionality. The value range is 10 to 172800. The default value is 120 seconds.</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets router port pruning time to 320 seconds.

(configure)# set intelligent-multicast router-port-pruning time 320

set intelligent-multicast session-pruning

Command Mode  Global Configuration.

Description  Enables or disables session pruning for Intelligent Multicasting. Intelligent multicast session pruning will remove any multicast session from configuration that has been determined to be inactive for a specified amount of time. By default, Intelligent Multicast session pruning is enabled.

Syntax

| To Enable:          | set intelligent-multicast session-pruning enable |
| To Disable:         | set intelligent-multicast session-pruning disable |

Sample Output  The following example disables intelligent-multicast session pruning.

(configure)# set intelligent-multicast session-pruning disable

set intelligent-multicast session-pruning time

**Command Mode**
Global Configuration.

**Description**
Sets the time interval after which inactive learned sessions are removed.

**Syntax**
set intelligent-multicast session-pruning time `<seconds>`

**Table 10-11. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td>The number of seconds that a dynamic Intelligent Multicast Session must be inactive before it is pruned by the Intelligent Multicast functionality. The value range is 10 to 172800. The default value is 250 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets intelligent-multicast session pruning time to 320 seconds.

```
(configure) # set intelligent-multicast session-pruning time 320
```

**Systems**
**set intelligent-multicast static-client-port**

**Command Mode**  
Global Configuration.

**Description**  
Adds a client port to a static Intelligent Multicast session.

**Syntax**  
```
set intelligent-multicast static-client-port {<group-address>|mac-address <mac-address>} vlan {all | <vlan-id> | name <vlan-name>} port <mod-port-spec>
```

**Table 10-12. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;group-address&gt;</td>
<td>The multicast IP address of a static multicast session</td>
</tr>
<tr>
<td>&lt;mac-address&gt;</td>
<td>The multicast MAC Address of a static non-IP multicast session.</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td></td>
<td>• all - All VLANS.</td>
</tr>
<tr>
<td></td>
<td>• vlan-id - The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td></td>
<td>• name - The VLAN name.</td>
</tr>
<tr>
<td>port</td>
<td>The client port in the multicast session. &lt;mod-port-spec&gt; is the port specifier for the static multicast client.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example assigns port 3.11 to a session for multicast group 229.10.10.10 on VLAN 4.

```
(configure)# set intelligent-multicast static-client-port 229.10.10.10 vlan 4 port 3/11
Multicast Client successfully created
```

**Systems**  
set intelligent-multicast static-session

**Command Mode**

Global Configuration.

**Description**

Creates an Intelligent Multicast session.

**Syntax**

```
set intelligent-multicast static-session { <group-address> | mac-address <mac-address> } vlan { all | <vlan-id> | name <vlan-name> }
```

**Table 10-13. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;group-address&gt;</td>
<td>The multicast IP address of the multicast session.</td>
</tr>
<tr>
<td>&lt;mac-address&gt;</td>
<td>The multicast MAC address of the non-IP multicast session.</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td></td>
<td>• <strong>all</strong> - All VLANS.</td>
</tr>
<tr>
<td></td>
<td>• <strong>vlan-id</strong> - The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td></td>
<td>• <strong>name</strong> - The VLAN name.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example sets an intelligent-multicast static session for multicast group 229.10.10.10 on a VLAN named *adams*.

```
(configure)# set intelligent-multicast static-session 229.10.10.10
vlan name adams
```

**Systems**

set lgmp client

Command Mode  Global Configuration.

Description  Enables or disables the LGMP client functionality. The default state is disabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set lgmp client enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set lgmp client disable</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables lgmp client.

(configure)# set lgmp client enable

**set lgmp server**

**Command Mode**  
Global Configuration.

**Description**  
Enables or disables the LGMP server. The LGMP server is disabled by default.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set lgmp server enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set lgmp server disable</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example disables lgmp server

```
(configure)# set lgmp server disable
```

**Systems**  
set lgmp server priority

Command Mode  Global Configuration.

Description  Sets the LGMP server ID priority. Excluding the parameter sets the priority to its default of 128.

Syntax  set lgmp server priority [<server-priority>]

Table 10-14. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;server-priority&gt;</td>
<td>Specifies the most significant byte of the LGMP Server ID. The lower four bytes are defined by the IP address of the interface and VLAN associated with the particular LGMP Server. The server priority can make LGMP servers on a device distributors or non-distributors. The lowest LGMP Server ID wins the distributor election. The range is 0 to 255.</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the LGMP server priority to 140.

```
(configure)# set lgmp server priority to 140
LGMP Server ID Priority successfully set to 140
```

set lgmp server proxy

**Command Mode**  
Global Configuration.

**Description**  
Enables or disables the LGMP server proxy mode. The proxy mode allows an LGMP server to generate LGMP Router Report and LGMP Router Leave messages on behalf of another router on the same VLAN. The default state is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set lgmp server proxy enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set lgmp server proxy disable</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example enables lgmp server proxy.

```
(configure)# set lgmp server proxy enable
LGMP Server Proxy Mode successfully set to enable
```

**Systems**  
set lgmp server router-report-time

Command Mode
Global Configuration.

Description
Sets the LGMP server router report time. Omitting the parameter sets the router report time to its default time of 125 seconds.

Syntax
set lgmp server router-report-time [<rrt-seconds>]

Sample Output
The following example sets the router report time to 150 seconds.

(configure)# set lgmp server router-report-time 150
LGMP Server Router Report Time successfully set to 150

Table 10-15. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;rrt-seconds&gt;</td>
<td>The router report time, measured in seconds, defines the interval in which the LGMP server distributor should send LGMP Router Report messages. These messages are used by the distributor election as a keep-alive for the current distributor. The range is 10 to 10000.</td>
</tr>
</tbody>
</table>

Systems
set lgmp server robust-variable

**Command Mode**  
Global Configuration.

**Description**  
Sets the LGMP server robustness variable. Omitting the parameter sets the robustness variable to its default value of 2.

**Syntax**  
set lgmp server robust-variable [<rv-val>]

**Table 10-16. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;rv-val&gt;</td>
<td>The robustness variable that defines the scalar used to calculate the timeout for an LGMP server non-distributor to become a distributor. The scalar is used to calculate non-distributor timeout. The range is 2 to 10.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the robustness variable to 4.

```
(configure)# set lgmp server robust-variable 4
LGMP Server Robustness Variable successfully set to 4
```

**Systems**  
show cgmp statistics

Command Mode
User.

Description
Displays CGMP-related statistics.

Syntax
show cgmp statistics [detailed]

Table 10-17. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[detailed]</td>
<td>Displays detailed cgmp statistics.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays cgmp statistics:

> show cgmp statistics
CGMP Snooping is currently disabled.

CGMP Packet Reception Stats
-----------------------------
Join Messages Received -------- 0
Leave Messages Received --------- 0
Unknown CGMP Messages Received --- 0

CGMP Action Stats
-------------------
New Sessions Created -------------- 0
New Client Ports Added ------------ 0
Existing Sessions Removed --------- 0
All Sessions Removed -------------- 0
New Router Ports Added ------------ 0
Existing Router Ports Removed ----- 0

Systems
show igmp-snooping statistics

Command Mode
User.

Description
Displays IGMP snooping configuration and statistics.

Syntax
show igmp-snooping statistics [detailed]

Table 10-18. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>

Sample Output
The following example shows the igmp-snooping statistics:

> show igmp-snooping statistics
IGMP Snooping is currently enabled.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Sessions Created</td>
<td>0</td>
</tr>
<tr>
<td>Sessions Destroyed</td>
<td>0</td>
</tr>
<tr>
<td>New Client Ports Added</td>
<td>0</td>
</tr>
<tr>
<td>New Router Ports Added</td>
<td>0</td>
</tr>
<tr>
<td>Router Ports Removed</td>
<td>0</td>
</tr>
</tbody>
</table>

Systems
**show intelligent-multicast client-port**

**Command Mode**  User.

**Description**  Displays current client ports that are assigned to a particular session.

**Syntax**  
```
show intelligent-multicast client-port <session-id>
```

**Table 10-19. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| `<session-id>` | The number assigned to the multicast session when it is created.  
This ID is displayed in the show intelligent-multicast session command. |

**Sample Output**  The following example displays the ports that are configured for Intelligent Multicasting on multicast session 4.

```plaintext
> show intelligent-multicast client-port 4
IM Client

Port Application
------------------
3.4 Router
6.1 Mgmt: 226.0.0.9

Systems
```
show intelligent-multicast configuration

Command Mode User.

Description Displays global configuration information for Intelligent Multicasting.

Syntax show intelligent-multicast configuration

Sample Output The following example shows the Intelligent Multicast configuration with the default values.

    > show intelligent-multicast configuration
    Intelligent Multicast Global Configuration
    ===============================================
    Enable State: Enable
    Automatic Router Port Pruning:
      Enable State: Enable
      Time : 120 Seconds
    Automatic Session Pruning:
      Enable State: Enable
      Time : 250 Seconds
    Automatic Client Pruning:
      Enable State: Disable
      Time : 60 Minutes

show intelligent-multicast router-port

Command Mode
User.

Description
Displays the Intelligent Multicast router ports.

Syntax
show intelligent-multicast router-port

Sample Output
The following example displays the router ports that are configured for Intelligent Multicast.

> show intelligent-multicast router-port
IM Router VLAN Port Name Applications
--------- ---- --------- --------------
 6.1  All   Mgmt
 6.3  All   Mgmt
 6.2  foo   Mgmt
 6.4  bar   Mgmt

Systems
show intelligent-multicast session

Command Mode
User.

Description
Displays Intelligent Multicast sessions that optionally match specified search criteria. Omitting any criteria displays all configured Intelligent Multicast sessions.

Syntax
show intelligent-multicast session [vlan {<vlan-id> | name <vlan-name>}] [{ip-address <group-address> <ip-mask> | {mac-address <wildcard-mac-address>}}] [client-port <mod-port-spec>]

Table 10-20. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>&lt;vlan-id&gt; is the VLAN ID of the session(s) to display.</td>
</tr>
<tr>
<td>name</td>
<td>&lt;vlan-name&gt; - The name of the VLAN of the session(s) to display.</td>
</tr>
<tr>
<td>ip-address</td>
<td>The IP address associated with the multicast session.</td>
</tr>
<tr>
<td></td>
<td>• group-address - The multicast IP address of the multicast group.</td>
</tr>
<tr>
<td></td>
<td>• ip-mask - The subnet mask used to determine which portions of &lt;group-address&gt; should be matched</td>
</tr>
<tr>
<td>mac-address</td>
<td>The MAC address associated with this entry:</td>
</tr>
<tr>
<td></td>
<td>• wildcard-mac-address - The multicast MAC address of the session(s) to display. The wildcard is indicated by a single asterisk (*) before the MAC address.</td>
</tr>
<tr>
<td>client-port</td>
<td>Switch port number that is a client port for an Intelligent Multicast session.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays information about all Intelligent Multicast sessions configured on the switch.

> show intelligent-multicast session

<table>
<thead>
<tr>
<th>ID</th>
<th>MAC Address</th>
<th>VLAN</th>
<th>Clients</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01:00:5E:01:01:02</td>
<td>Default</td>
<td>1</td>
<td>Mgmt:</td>
</tr>
<tr>
<td>2</td>
<td>01:00:5E:01:01:02</td>
<td>Default</td>
<td>1</td>
<td>Mgmt:</td>
</tr>
<tr>
<td>2</td>
<td>01:00:5E:01:01:02</td>
<td>Adams</td>
<td>1</td>
<td>Mgmt: 255.1.1.2</td>
</tr>
<tr>
<td>3</td>
<td>01:00:5E:01:01:02</td>
<td>Alcott</td>
<td>0</td>
<td>Mgmt: 256.0.0.9</td>
</tr>
</tbody>
</table>

Systems
**show intelligent-multicast static-client**

**Command Mode**  
User.

**Description**  
Displays all statically configured client ports for a given Intelligent Multicast session.

* Note: If a static session is created with `vlan all`, then you must specify `vlan all` to see the clients. If a static session is created with an IP address, then you cannot use the MAC address to see the clients.

**Syntax**  
```
show intelligent-multicast static-client { <group-address> | mac-address <mac-address>} vlan {all | <vlan-id> | name <vlan-name>}
```

**Table 10-21. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;group-address&gt;</code></td>
<td>The IP address of the multicast group.</td>
</tr>
<tr>
<td><code>&lt;mac-address&gt;</code></td>
<td>The MAC address associated with this entry:</td>
</tr>
<tr>
<td><code>vlan</code></td>
<td>The choices are:</td>
</tr>
<tr>
<td></td>
<td>• <code>all</code> - The static session or client is created for all VLANS.</td>
</tr>
<tr>
<td></td>
<td>• <code>vlan-id</code> - A session or client is created for a specific VLAN only identified by numerical ID.</td>
</tr>
<tr>
<td></td>
<td>• <code>name</code> - A session or client is created for a specific VLAN only identified by VLAN name.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example displays the Intelligent Multicast client ports for the multicast session created with all VLANS.

```plaintext
> show intelligent-multicast static-client 225.1.1.2 vlan all
IM          ClientPort   Application
-----------------          ---------------
1      3.2               Mgmt : 225.1.1.2
```

**Systems**  
show intelligent-multicast static-session

**Command Mode**
User.

**Description**
Displays all manually configured sessions for Intelligent Multicasting.

**Syntax**
show intelligent-multicast static-session

**Sample Output**
The following example displays the Intelligent Multicast static sessions.

> show intelligent-multicast static-session

<table>
<thead>
<tr>
<th>VLAN</th>
<th>MAC Address</th>
<th>IP Address</th>
<th># Clients</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>01:00:5E:01:01:02</td>
<td>225.1.1.2</td>
<td>1</td>
</tr>
<tr>
<td>All</td>
<td>01:00:5E:01:04:05</td>
<td>225.1.4.5</td>
<td>0</td>
</tr>
<tr>
<td>All</td>
<td>01:00:5E:00:00:09</td>
<td>226.0.0.9</td>
<td>1</td>
</tr>
</tbody>
</table>

**Systems**
**show lgmp client**

**Command Mode** User.

**Description** Displays current LGMP client configuration information or statistics. Omitting parameters after the statistics keyword displays global LGMP client statistics.

**Syntax**

```
show lgmp client {config | statistics [vlan {all | <vlan-id> | name <vlan-name>}]}
```

**Table 10-22. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>LGMP client configuration or statistics.</td>
</tr>
<tr>
<td>statistics</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td>all</td>
<td>- All VLANS.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>- The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td>name &lt;vlan-name&gt;</td>
<td>- The VLAN name.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example displays LGMP client statistics.

```
> show lgmp client statistics
Global LGMP Client Statistics

LGMP Client Message Reception Stats

<table>
<thead>
<tr>
<th>Report</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaf</td>
<td>0</td>
</tr>
<tr>
<td>End Session</td>
<td>0</td>
</tr>
<tr>
<td>Router Report</td>
<td>0</td>
</tr>
<tr>
<td>Router Leave</td>
<td>0</td>
</tr>
<tr>
<td>Invalid</td>
<td>0</td>
</tr>
</tbody>
</table>

LGMP Client Intelligent Multicast Session Stats

<table>
<thead>
<tr>
<th>New Client Ports Added</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Client Ports Removed</td>
<td>0</td>
</tr>
<tr>
<td>Existing Sessions Removed</td>
<td>0</td>
</tr>
<tr>
<td>New Router Ports Added</td>
<td>0</td>
</tr>
<tr>
<td>ExistingRouter Ports Removed</td>
<td>0</td>
</tr>
</tbody>
</table>
```

show lgmp server

Command Mode  User.

Description  Displays current LGMP server configuration information or statistics. Omitting parameters after the statistics keyword displays global LGMP server statistics.

Syntax  

```
show lgmp server {config | statistics [vlan {all | <vlan-id> | name <vlan-name>}]}
```

Sample Output  The following example shows the LGMP server statistics:

```
> show lgmp server statistics
Global LGMP Server Statistics
=================================
LGMP Server Message Reception Stats
===================================
    Router Report -------------------- 0
    Invalid -------------------------- 0
LGMP Server Message Transmission Stats
======================================
    Report --------------------------- 0
    Leave ---------------------------- 0
    End Session ---------------------- 0
    Router Report -------------------- 0
    Router Leave --------------------- 0
LGMP Server Intelligent Multicast Session Stats
======================================
    Client Ports Added --------------- 0
    Client Ports Removed ------------- 0
    Sessions Removed ----------------- 0
    Router Ports Added --------------- 0
    Router Ports Removed ------------- 0
```

Table 10-23. Parameters, Keywords, Argument

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>statistics</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td>all</td>
<td>All VLANS.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td>name</td>
<td>The VLAN name.</td>
</tr>
</tbody>
</table>

Overview

This chapter describes the following commands:

- **arp**
- **arp timeout**
- **clear arp-cache**
- **clear ip route**
- **clear tcp**
- **interface**
- **ip address**
- **ip admin-state**
- **ip bootp-dhcp agent-info**
- **ip bootp-dhcp circuit-info**
- **ip bootp-dhcp relay**
- **ip bootp-dhcp server**
- **ip default-gateway**
- **ip directed broadcast**
- **ip domain-list**
- **ip domain-lookup**
- **ip domain-name**
- **ip http**
- **ip irdp**
- **ip irdp holdtime**
- **irdp maxadvertinterval**
- **ip irdp minadvertinterval**
- ip irdp multicast
- ip irdp preference
- ip mac-format
- ip max-arp-entries
- ip max-route-entries
- ip multicast-routing
- ip name-server
- ip netbios-rebroadcast
- ip netmask-format
- ip proxy-arp
- ip proxy-arp-default-route
- ip proxy-arp-limit
- ip redirects
- ip reset-stats
- ip route
- ip route-preference
- ip routing
- ip routing-mode
- ip short-lived
- ip source-route
- ip telnet inactivity-period
- ip telnet
- ip vlan
- ping
- redistribute
- show arp
- show hosts
- show ip arp
- show ip interface
- show ip irdp
- show ip redistribute
- show ip route
- show ip route summary
- show ip short-lived
- show ip traffic
- show tcp configuration
- show tcp connections
- show tcp statistics
- show udp statistics
Chapter 11

arp

**Command Mode**
Global Configuration.

**Description**
Creates a permanent entry in the Address Resolution Protocol (ARP) table. The no form of this command deletes an entry.

**Syntax**

| To Create: | arp <ip-address> <hw-addr> |
| To Delete: | [no] arp <ip-address> <hw-addr> |

**Table 11-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IP address, in dotted decimal format, of the local data link.</td>
</tr>
<tr>
<td>&lt;hw-addr&gt;</td>
<td>48-bit address of the local data link.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example adds a permanent entity to the ARP cache at IP address 10.10.10.1, and the hardware-address 00:01:0D:00:35:45.

```
(configure)# arp 10.10.10.1 00:01:0D:00:35:45
```

**Systems**
arp timeout

Command Mode

Interface Configuration.

Description

Configures the amount of time that an entry remains in the ARP cache on an interface. The no form of this command restores the default value.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>arp timeout &lt;seconds&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] arp timeout</td>
</tr>
</tbody>
</table>

Table 11-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;seconds&gt;</td>
<td>The amount of time, in seconds, that an entry remains in the arp cache</td>
</tr>
</tbody>
</table>

Sample Output

The following example sets the arp timeout period to 300 seconds on an interface labeled “boston”.

    (config-if:boston)# arp timeout 300

Systems

clear arp-cache

Command Mode  Global Configuration.

Description  Deletes all dynamic entries from the ARP cache.

Syntax  clear arp-cache

Sample Output  The following example clears all dynamic entries from the ARP cache:

    (configure) # clear arp-cache

clear ip route

**Command Mode**  
Global Configuration.

**Description**  
Deletes routes from the IP routing table.

**Syntax**  
clear ip route {<network> [<mask>] | *}

**Table 11-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;network&gt;</td>
<td>The network or subnet address to remove.</td>
</tr>
<tr>
<td>[&lt;mask&gt;]</td>
<td>Subnet address to remove.</td>
</tr>
<tr>
<td>*</td>
<td>Clears all routes.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example deletes ip routes from the network with an IP address of 10.10.10.0 and the mask of 255.255.0.0,

```
(configure)# clear ip route 10.10.10.0 255.255.0.0
```

**Systems**  
clear tcp

Command Mode Global Configuration.

Description Ends the TCP session that you specify.

Syntax clear tcp [all | local <local-ip-address> <local-tcp-port> remote <remote-ip-address> <remote-tcp-port>]

Table 11-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Ends all TCP sessions on the switch.</td>
</tr>
<tr>
<td>local</td>
<td>Ends a specific TCP session on the local switch.</td>
</tr>
<tr>
<td>&lt;local-ip-address&gt;</td>
<td>The local IP address for which you want to end the TCP session.</td>
</tr>
<tr>
<td>&lt;local-tcp-port&gt;</td>
<td>The local TCP port number for which you want to end the TCP session.</td>
</tr>
<tr>
<td>remote</td>
<td>The associated TCP session on the remote switch.</td>
</tr>
<tr>
<td>&lt;remote-ip-address&gt;</td>
<td>The associated remote IP address for which you want to end the TCP session.</td>
</tr>
<tr>
<td>&lt;remote-tcp-port&gt;</td>
<td>The associated remote TCP port number for which you want to end the TCP session.</td>
</tr>
</tbody>
</table>

**interface**

**Command Mode**  Global Configuration.

**Description**  Configures an interface type and enters Interface Configuration mode. The **no** form of this command deletes an interface with the name specified.

To enter Interface Configuration mode, omit the [type {nbma | ethernet}] option.

**Syntax**

| To Configure: | interface <intf-name> [type {nbma | ethernet}] |
|---------------|-----------------------------------------------|
| To Delete:    | [no] interface <intf-name>                   |

**Table 11-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;intf-name&gt;</td>
<td>A name for the interface you are attempting to configure or create. This name can be series of characters from 1 - 32 characters long.</td>
</tr>
<tr>
<td>nbma</td>
<td>Sets the interface to be a non-broadcast multi-access (NBMA) IP interfaces. NBMA interfaces make it possible for the switch to exchange routing information over nonbridged connections (routed virtual switch ports (VSPs)) NBMA functionality was added to RIP and OSPF routing protocols on the Avaya Multiservice switch software</td>
</tr>
<tr>
<td>ethernet</td>
<td>Sets the interface to be an ethernet LAN interface.</td>
</tr>
</tbody>
</table>

ip address

Command Mode
Interface Configuration.

Description
Assigns an IP address to an interface. To remove an IP address or disable IP processing, use the no form of this command.

Syntax

<table>
<thead>
<tr>
<th>To Assign:</th>
<th>ip address &lt;ip-address&gt; &lt;mask&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Remove:</td>
<td>no ip address &lt;ip-address&gt; &lt;mask&gt;</td>
</tr>
</tbody>
</table>

Table 11-6. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>The IP address assigned to the interface.</td>
</tr>
<tr>
<td>&lt;mask&gt;</td>
<td>Mask for the associated IP subnet.</td>
</tr>
</tbody>
</table>

Sample Output
The following example assigns IP address 170.180.5.33 to an interface labeled “boston”.

(config-if:boston)# ip address 170.180.5.33

Systems
**ip admin-state**

**Command Mode**
Interface Configuration.

**Description**
Sets the administrative state of an IP interface. The default state is **up**.

**Syntax**
`ip admin-state {up | down}`

---

**Table 11-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{up</td>
<td>down}</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the administrative state of an interface labeled “boston” to up.

```
(config-if:boston)# ip admin-state up
```

**Systems**
**ip bootp-dhcp agent-info**

**Command Mode**  
Global Configuration.

**Description**  
Enables BOOTP/DHCP option 82, suboption 2 (agentID). The no command disables option 82, suboption 2.

This suboption identifies the IP address and, if available, the system name of the switch. The default setting is disabled.

*Note:* Before you enter this command, make sure that the switch is set to be a BOOTP/DHCP relay agent. Use the `ip bootp-dhcp relay` command to enable BOOTP/DHCP relay agent on the switch.

**Syntax**

<table>
<thead>
<tr>
<th><strong>To Enable:</strong></th>
<th>ip bootp-dhcp agent-info</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Disable:</strong></td>
<td>no ip bootp-dhcp agent-info</td>
</tr>
</tbody>
</table>

**Systems**  
ip bootp-dhcp circuit-info

**Command Mode**
Global Configuration.

**Description**
Enables BOOTP/DHCP option 82, suboption 1 (circuitID). The *no* command disables option 82, suboption 1.

This suboption identifies the slot and physical port number from which the DHCP request was received. The default setting is disabled.

*Note:* Before you enter this command, make sure that the switch is set to be a BOOTP/DHCP relay agent. Use the `ip bootp-dhcp relay` command to enable BOOTP/DHCP relay agent on the switch.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip bootp-dhcp circuit-info</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip bootp-dhcp circuit-info</td>
</tr>
</tbody>
</table>

**Systems**
**ip bootp-dhcp relay**

**Command Mode**
Global Configuration.

**Description**
Enables relaying BOOTP and DHCP service to the BOOTP/DHCP server. The **no** command disables relaying BOOTP and DHCP service to the BOOTP/DHCP server. The default setting is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip bootp-dhcp relay</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip bootp-dhcp relay</td>
</tr>
</tbody>
</table>

**Systems**
**ip bootp-dhcp server**

**Command Mode**
Global Configuration.

**Description**
Adds a BOOTP/DHCP server entry. The `no` command removes the BOOTP/DHCP server entry.

When you add a BOOTP/DHCP server entry, the switch serves as a BOOTP/DHCP relay agent between the BOOTP/DHCP server and the requesting client.

*Note:* Before you enter this command, make sure that the switch is set to be a BOOTP/DHCP relay agent. Use the `ip bootp-dhcp relay` command to enable BOOTP/DHCP relay agent on the switch.

**Syntax**

<table>
<thead>
<tr>
<th>To Add:</th>
<th>ip bootp-dhcp server <code>&lt;ip-address&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Remove:</td>
<td><code>[no] ip bootp-dhcp server </code>&lt;ip-address&gt;``</td>
</tr>
</tbody>
</table>

**Table 11-8. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>IP address of the BOOTP/DHCP server for which you want to add an entry.</td>
</tr>
</tbody>
</table>

**Systems**
ip default-gateway

**Command Mode**
Global Configuration.

**Description**
Defines a default gateway (router) when IP routing is disabled. The no form of this command removes a default gateway. The default state is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip default-gateway &lt;ip-address&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip default-gateway &lt;ip-address&gt;</td>
</tr>
</tbody>
</table>

**Table 11-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IP address of the router.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example defines the router at address 128.88.84.34 as the default gateway.

```none
(configure)# ip default-gateway 128.88.84.34
```

**Systems**
ip directed broadcast

**Command Mode**  
Interface Configuration.

**Description**  
When the IP Directed-Broadcast feature is enabled, it allows a net-directed broadcast (unicast IP address with the host ID set to all ones) to be forwarded by the router on the selected interface. The default setting is enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip directed-broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip directed-broadcast</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example enables directed-broadcast on the interface labeled “boston”.

```
(config-if:boston)# ip directed-broadcast
```

**Systems**  
**ip domain-list**

**Command Mode**
Global Configuration.

**Description**
Defines a default domain name to complete unqualified host names. You can define a maximum of six default domain names. The **no** form of this command removes the domain name.

**Syntax**

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Add:</strong></td>
<td><code>ip domain-list &lt;name&gt;</code></td>
</tr>
<tr>
<td><strong>To Remove:</strong></td>
<td><code>no ip domain-list &lt;name&gt;</code></td>
</tr>
</tbody>
</table>

**Sample Output**
The following example adds the name “avaya.com” to the DNS name list.

```
(configure) # ip domain-list avaya.com
```

**Systems**
ip domain-lookup

Command Mode  Global Configuration.

Description  Enables DNS client. The no form of this command disables DNS client.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip domain-lookup</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip domain-lookup</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables DNS.

(configure)# ip domain-lookup

**ip domain-name**

**Command Mode**
Global Configuration.

**Description**
Defines a default domain name to complete unqualified host names. You can define a maximum of six default domain names. The **no** form of this command removes the domain name.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip domain-name &lt;domain-name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip domain-name &lt;domain-name&gt;</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example adds the name “avaya.com” to the DNS name list.

```
(configure) # ip domain-name avaya.com
```

**Systems**
**ip http**

**Command Mode**  
Global Configuration.

**Description**  
Enables or disables HTTP and changes the port number for HTTP. Valid port numbers are 80 or a port number from 9000 through 65535. The default setting is port 80.

Once you change the TCP port number for HTTP, only users who know the new port number can access the Web Agent.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th><code>ip http {port [&lt;tcp-new-port&gt;] [enable] [enable]}</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td><code>no ip http</code></td>
</tr>
</tbody>
</table>

**Table 11-10. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;tcp-new-port&gt;</code></td>
<td>The TCP port number that you want to use for HTTP requests. The default setting is port 80. Valid port numbers are 80 or a port number from 9000 through 65535. Once you change the TCP port number for HTTP, only users who know the new port number can access the Web Agent.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables HTTP.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example changes the TCP port for HTTP requests to port 9999:

```
(configure)# ip http port 9999
TCP HTTP listening port was changed successfully to 9999
```

**Systems**  
**ip irdp**

**Command Mode**
Interface Configuration.

**Description**
Enables the ICMP Router Discovery Protocol (IRDP) on an interface. The no form of this command restores the default, which is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip irdp</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip irdp</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables IRDP on IP Interface labeled “boston”.

```
(config-if:boston)# ip irdp
```

**Systems**
ip irdp holdtime

**Command Mode**
Interface Configuration.

**Description**
Sets the length of time, in seconds, that advertisements are held valid. The holdtime value must be greater than the maxadvertinterval value and cannot be greater than 9000 seconds. The range is 5 - 9000 seconds. The default is 1800 seconds.

The **no** command restores the default setting.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip irdp holdtime &lt;irdpHoldTime&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip irdp holdtime</td>
</tr>
</tbody>
</table>

**Table 11-11. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;irdpHoldTime&gt;</td>
<td>The length of time, in seconds, that advertisements are held valid.</td>
</tr>
<tr>
<td></td>
<td>The holdtime value must be greater than the maxadvertinterval value and cannot be greater than 9000 seconds. The range is 5 - 9000 seconds. The default is 1800 seconds.</td>
</tr>
</tbody>
</table>

**Systems**
**irdp maxadvertinterval**

**Command Mode**  
Interface Configuration.

**Description**  
Sets the maximum interval in seconds between advertisements. The range is 4 to 1800 seconds. The default value is 600 seconds.

The **no** command restores the default setting.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip irdp maxadvertinterval &lt;irdpMaxTimer&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip irdp maxadvertinterval</td>
</tr>
</tbody>
</table>

**Table 11-12. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;irdpMaxTimer&gt;</td>
<td>Maximum interval in seconds between advertisements. The range is 4 - 1800 seconds. The default value is <strong>600</strong> seconds.</td>
</tr>
</tbody>
</table>

**Systems**  
ip irdp minadvertinterval

Command Mode

Interface Configuration.

Description

Sets the minimum interval in seconds between advertisements. The range is 3 to 1799 seconds. The default setting is 450 seconds. Changing the maxadvertinterval value automatically changes the minadvertinterval value to three-quarters of the new value.

The no command restores the default setting.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip irdp minadvertinterval &lt;irdpMinTimer&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip irdp minadvertinterval</td>
</tr>
</tbody>
</table>

Table 11-13. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;irdpMinTimer&gt;</td>
<td>The minimum interval in seconds, between advertisements.</td>
</tr>
<tr>
<td></td>
<td>The range is 3 to 1799 seconds.</td>
</tr>
<tr>
<td></td>
<td>The default setting is 450 seconds.</td>
</tr>
</tbody>
</table>

Systems

ip irdp multicast

**Command Mode**
Interface Configuration.

**Description**
Sets the router discovery addressing mode. Forces this interface to send advertisements to the multicast address (224.0.0.1) instead of IP broadcast address (255.255.255.255).

The `no` command forces the interface to use the IP broadcast address.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip irdp multicast</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip irdp multicast</td>
</tr>
</tbody>
</table>

**Systems**
ip irdp preference

Command Mode
Global Configuration.

Description
Sets the preference of the address as a default router address, relative to other router addresses on the same subnet. The minimum value (80000000 hex) is used to indicate that the address should not be used by neighboring hosts as a default router address, even though it may be advertised. The default setting is 0.

The no command restores the default setting.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip irdp preference &lt;irdp-pref-num&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip irdp preference</td>
</tr>
</tbody>
</table>

Table 11-14. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;irdp-pref-num&gt;</td>
<td>The preference of the address as a default router address, relative to other router addresses on the same subnet. The minimum value (80000000 hex) is used to indicate that the address should not be used by neighboring hosts as a default router address, even though it may be advertised. The default value is 0.</td>
</tr>
</tbody>
</table>

Systems
ip mac-format

Command Mode  
Interface Configuration.

Description  
Sets the MAC format of the IP interfaces. The no form of this command restores the default ethv2.

Syntax

| To Configure:          | ip mac-format {ethv2 | snap}                |
|------------------------|---------------------------------|
| To Restore Default:    | no ip mac-format {ethv2 | snap}                |

Table 11-15. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ethv2</td>
<td>snap}</td>
</tr>
</tbody>
</table>

Sample Output

The following example sets the MAC format of the IP interfaces, on the interface labeled boston, to the Subnetwork Access Protocol (snap).

(config-if:boston)# ip mac-format snap

Systems

**ip max-arp-entries**

**Command Mode**  
Global Configuration.

**Description**  
Specifies the maximum number of ARP cache entries allowed in the ARP cache. The default maximum number of entries is 16,384. The no command restores the default setting.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip max-arp-entries &lt;value&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip max-arp-entries</td>
</tr>
</tbody>
</table>

**Table 11-16. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;value&gt;</td>
<td>The space that is available for the ARP cache. When you increase the number of entries, it may cause the table to be relearned more frequently, thus increasing address space. The default maximum number of entries is 16,384.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example specifies the maximum number of ARP cache entries allowed in the ARP cache to 100.

```
(configure)# ip max-arp-entries 100
```

**Systems**  
**ip max-route-entries**

**Command Mode**  
Global Configuration.

**Description**  
Specifies the maximum number of routes that can be added to the routing table. These routes refer to IP Unicast entries only. The default number of routes is 16,384. The **no** command restores the default setting.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip max-route-entries &lt;value&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip max-route-entries</td>
</tr>
</tbody>
</table>

**Table 11-17. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;value&gt;</td>
<td>The space that is available for the IP address table. When you increase the number of entries, it may cause the table to be relearned more frequently, thus increasing address space.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example specifies the number of routes that can be added to the routing table as 50.

```
(configure)# ip max-route-entries 50
```

**Systems**  
ip multicast-routing

**Command Mode**
Global Configuration.

**Description**
Globally enables IP multicast routing. IP multicast routing must be enabled to configure IGMP or DVMRP. The no form of this command disables IP multicast routing. The default state is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip multicast-routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip multicast-routing</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables IP multicast routing.

```
(configure)# ip multicast-routing
```

**Systems**
ip name-server

Command Mode  Global Configuration.

Description  Adds a DNS server address. The no form of this command removes the DNS server address.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip name-server &lt;ip address&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip name-server &lt;ip address&gt;</td>
</tr>
</tbody>
</table>

Sample Output  The following example adds the DNS address 210.120.87.90.

(configure) # ip name-server 210.120.87.90

ip netbios-rebroadcast

**Command Mode**
Interface Configuration.

**Description**
Enables NETBIOS rebroadcasts on an interface. The **no** form of this command disables NETBIOS rebroadcasts on an interface (default).

**Syntax**

| To Enable:         | ip netbios-rebroadcast [{both | inbound | outbound | disable}] |
|--------------------|-----------------------------------------------------------|
| To Disable:        | no ip netbios-rebroadcast                                 |

**Table 11-18. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{both</td>
<td>inbound</td>
</tr>
<tr>
<td></td>
<td>• <strong>both</strong> - inbound and outbound broadcasts are accepted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>inbound</strong> - only inbound broadcasts are accepted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>outbound</strong> - only outbound broadcasts are accepted.</td>
</tr>
<tr>
<td></td>
<td>• <strong>disable</strong> - no broadcasts are accepted.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables NETBIOS rebroadcasts and accepts only INBOUND broadcasts on an interface labeled “boston”.

```
(config-if:boston)# ip netbios-rebroadcast inbound
```

**Systems**
ip netmask-format

Command Mode
Global Configuration.

Description
Specifies the format of netmasks in the show command output. The no form of this command restores the default, which is a dotted decimal format.

Syntax

| To Configure: | ip netmask-format {bitcount | decimal | hexadecimal} |
|---------------|--------------------------------------------------------|
| To Restore Default: | no ip netmask-format |

Table 11-19. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{bitcount</td>
<td>decimal</td>
</tr>
<tr>
<td></td>
<td>• bitcount - Addresses are followed by a slash and the total number of bits in the netmask. For example, 131.108.11.0/24 indicates the netmask is 24 bits.</td>
</tr>
<tr>
<td></td>
<td>• decimal - The network masks are in dotted decimal notation. For example, 255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td>• hexadecimal - The network masks are in hexadecimal format as indicated by the leading 0X. For example, 0xFFFFF00.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays netmasks in bitcount format.

(configure)# ip netmask-format bitcount

Systems
**ip proxy-arp**

**Command Mode**  
Interface Configuration.

**Description**  
Enables proxy ARP on an interface. The **no** form of this command disables proxy ARP on an interface. The default state is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip proxy-arp</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip proxy-arp</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example disables proxy ARP on IP interface Boston.

```
(config-if:boston)# no ip proxy arp
```

**Systems**  
ip proxy-arp-default-route

**Command Mode**
Global Configuration.

**Description**
Enables use of the default route as the route for proxy ARPs. The `no` command disables use of the default route as the route for proxy ARPs. The default setting is enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip proxy-arp-default-route</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip proxy-arp-default-route</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables use of the default route for proxy ARPs.

```
(configure) # ip proxy-arp-default-route
```

**Systems**
ip proxy-arp-limit

Command Mode  Global Configuration.

Description  Enables proxy ARP. When enabled, the router only responds to ARP requests when the source and target IP address are in the same IP network and different IP subnets.

When disabled, the router only responds to ARP requests when the source and target IP address are in different networks. The no form of this command restores the default, which is disabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip proxy-arp-limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip proxy-arp-limit</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables proxy ARP.

(configure)# ip proxy-arp-limit

ip redirects

**Command Mode**
Interface Configuration.

**Description**
Enables the sending of redirect messages when the router is forced to resend a packet through the same interface on which it was received. The no form of this command disables the sending of redirect messages. The default state is enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip redirects</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip redirects</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables the sending of redirect messages on interface labeled “boston”.

```
(config-if:boston)# ip redirects
```

**Systems**
**ip reset-stats**

**Command Mode**
Global Configuration.

**Description**
Resets the IP statistics.

**Syntax**
ip reset-stats

**Sample Output**
The following example resets the IP statistics.

```
(configure)# ip reset-stats
```

**Systems**
**ip route**

**Command Mode**
Global Configuration.

**Description**
Creates a static route. The **no** form of this command removes a static route. The default static routing preference is Low.

**Syntax**

| To Create: | route <route-addr> <mask> {<next-hop> | null 0} <cost> [[high | low]] |
| --- | --- |
| To Delete: | no ip route <route-addr> <mask> |

**Table 11-20. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;route-addr&gt;</td>
<td>IP address of the static route.</td>
</tr>
<tr>
<td>&lt;mask&gt;</td>
<td>Mask of the IP address.</td>
</tr>
<tr>
<td>&lt;next-hop&gt;</td>
<td>The IP address for the gateway associated with the static route.</td>
</tr>
<tr>
<td>null 0</td>
<td>Creates a static route to a null interface. A null interface is a virtual interface that discards IP packets and is used to prevent routing loops from occurring in the network. For more information on null interfaces, see Chapter 12, “Configuring IP Routing,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
<tr>
<td>&lt;cost&gt;</td>
<td>The metric between this router and the destination. The cost can range from 1 to 65,535.</td>
</tr>
<tr>
<td>[[high</td>
<td>low]]</td>
</tr>
</tbody>
</table>
Sample Output

The following example establishes a static route on ip address 10.10.10.1, mask 255.255.0.0 with a next hop address of 10.15.1.1 and a low path cost.

(configure)# ip route 10.10.10.1 255.255.0.0 10.15.1.1 low

Systems

P580 and P882.
**ip route-preference**

**Command Mode**
Global Configuration.

**Description**
Assigns preference values to routes. The IP routing table uses these values to determine the best routes. The no form of this command restores the default settings.

**Syntax**

| To Configure:                  | ip route-preference {local | rip | ospf-intra | ospf-inter | ospf-extra | static-hp | static-lp} <value> |
|--------------------------------|--------------------------------------------------------------------------------|
| To Restore Default:            | [no] ip route-preference {local | rip | ospf-intra | ospf-inter | ospf-extra | static-hp | static-lp} |

**Table 11-21. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{local</td>
<td>rip</td>
</tr>
<tr>
<td></td>
<td>• <strong>local</strong> - locally connected routes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>rip</strong> - route learned via the RIP protocol.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ospf-intra</strong> - OSPF intra-area routes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ospf-extra</strong> - OSPF external routes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>static-hp</strong> - high preference static routes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>static-lp</strong> - low preference static routes.</td>
</tr>
<tr>
<td>&lt;value&gt;</td>
<td>Preference value assigned to the specified route. The higher the value, the more preferable the route. Valid preference values range from 0 to 255.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following sample assigns a preference of 100 to RIP routes.

```
(configure)# ip route-preference rip 100
```

**Systems**
ip routing

Command Mode  Global Configuration.

Description  Enables IP routing. The no form of this command disables IP routing. The default state is enabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip routing</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables IP routing.

(configure)# ip routing

ip routing-mode

**Command Mode**  Interface Configuration.

**Description**  Sets the IP routing mode on an interface. The no form of this command restores the default setting of RT_MGMT.

**Syntax**

| To Configure: | ip routing-mode {RT_MGMT | RT_ONLY | MGMT_ONLY} |
|---------------|----------------------------------|
| To Restore Default: | no ip routing-mode |

**Table 11-22. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| {RT_MGMT | RT_ONLY | MGMT_ONLY} | • **Routing/Mgmt** - IP routing is enabled on the interface, and you can manage the switch through the interface (from the CLI or Web Agent).
| | • **Mgmt Only** - You can manage the switch through the interface (from the CLI or Web Agent), but IP routing is disabled on the interface.
| | • **Routing Only** - Routing only interfaces do not permit management traffic destined for local interfaces but do allow all other traffic including management traffic destined for interfaces on other switches.  
| | **Note:** Do not enable routing protocols on an interface configured for Mgmt Only since the interface will act as an end point and will not pass traffic. |

**Sample Output**  This example enables local packet consumption and disables IP forwarding on an interface labeled “boston”.

```
(config-if:boston)# ip routing-mode MGMT_ONLY
```

ip short-lived

Command Mode  Global Configuration

Description  Enables a filter for a short-lived IP protocol.

Syntax

| To Enable:       | ip short-lived {tcp | udp} <port> |
|------------------|---------------------------------|
| To Disable:      | no ip short-lived {tcp | udp} <port> |

<table>
<thead>
<tr>
<th>Keyword, Argument, or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{tcp</td>
<td>udp}</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td>The TCP or UDP port number that the protocol uses. Enter a port number from 0 through 65535.</td>
</tr>
</tbody>
</table>

Sample Output

To send all SNMP packets to supervisor module for slow path routing, enter the following command:

```
(configure)# ip short-lived udp 161
```

To send all BOOTP and DHCP packets to the supervisor for slow path routing, enter the following commands:

```
(configure)# ip short-lived udp 67  
(configure)# ip short-lived udp 68
```

Systems  P580 and P882.
ip source-route

**Command Mode**
Global Configuration.

**Description**
Allows the router to handle IP datagrams with source-routing header options. The no form of this command discards any IP datagrams containing a source-route option. The default state is enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip source-route</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip source-route</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example specifies that the router discards IP datagrams with source-routing header options.

```plaintext
(configure)# no ip source-route
```

**Systems**
ip telnet inactivity-period

**Command Mode**
Global Configuration.

**Description**
Sets the IP telnet inactivity period. Specifies how many seconds a telnet session is to remain open with no activity. The default is 900 seconds, or 15 minutes. The `no` command restores the default setting.

Setting this command to 0 disables the timer so that sessions never close because of inactivity.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip telnet inactivity-period <code>&lt;timeout&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip telnet inactivity-period</td>
</tr>
</tbody>
</table>

**Table 11-24. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;timeout&gt;</code></td>
<td>The telnet inactivity timeout period, measured in seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the ip telnet inactivity timeout period to 800 seconds.

```
(configure)# ip telnet inactivity-period 800
```

**Systems**


**ip telnet**

**Command Mode**  
Global Configuration

**Description**  
Enables or disables Telnet and changes the TCP port number for Telnet. Valid port numbers are 23 or a port number from 9000 through 65355.

Once you change the TCP port number for Telnet, only users who know the new port number can start Telnet sessions to the switch.

<table>
<thead>
<tr>
<th><strong>To Enable:</strong></th>
<th>ip telnet {port [&lt;tcp-new-port&gt;] [enable]}</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Disable:</strong></td>
<td>no ip telnet</td>
</tr>
</tbody>
</table>

**Table 11-25. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;tcp-telnet-port&gt;</code></td>
<td>The TCP port number that you want to use for Telnet requests. The default setting is port 23. Valid port numbers are 23 or a port number from 9000 through 65355. Once you change the TCP port number for Telnet, only users who know the new port number can start Telnet sessions to the switch.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example changes the TCP port for Telnet requests to port 9998:

```
(configure)# ip telnet port 9998
TCP Telnet listening port was changed successfully to 9998
```

**Systems**  
**ip vlan**

**Command Mode**  
Interface Configuration.

**Description**  
Specifies the VLAN on which an IP interface resides. The no form of this command sets the IP interface to the Discard vlan.

**Syntax**

| To Enable: | ip vlan { <vlan-id> | name <vlan-name> | Ethernet-Console | Serial-Console } |
|------------|--------------------------------------------------|
| To Disable: | [no] ip vlan                                       |

**Table 11-26. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>ID of the VLAN.</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>Name of the VLAN.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example specifies that the interface labeled “boston” resides on VLAN 100

```
(config-if:boston)# ip vlan 100
```

**Systems**  
Chapter 11

ping

Command Mode
Privileged.

Description
Checks host reachability and network connectivity.

Syntax
ping <ip-addr> [<count> [<delay> [<size> [<timeout> [<quiet>]]]]]]

Sample Output
The following example checks the host reachability and host connectivity to
the host at IP address 192.168.0.115.

> ping 192.168.0.115
#1: Ping ok, RTT 0.000 seconds
#2: Ping ok, RTT 0.000 seconds
#3: Ping ok, RTT 0.000 seconds
#4: Ping ok, RTT 0.000 seconds
#5: Ping ok, RTT 0.000 seconds
Ping of 192.168.0.115 completed: 5 OK, 0 Failed

Table 11-27. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>IP address of the target system.</td>
</tr>
<tr>
<td>&lt;count&gt;</td>
<td>The number of ping attempts you want to perform with this operation. The default is 5.</td>
</tr>
<tr>
<td>&lt;delay&gt;</td>
<td>The number of milliseconds the switch waits between generating pings. the default is 1.</td>
</tr>
<tr>
<td>&lt;size&gt;</td>
<td>The size of the packet sent during a ping operation (0-1472).</td>
</tr>
<tr>
<td>&lt;timeout&gt;</td>
<td>The number of seconds to wait for an ICMP reply. The default is 2.</td>
</tr>
<tr>
<td>quiet</td>
<td>Include this keyword to disable the display of the ping operation in progress.</td>
</tr>
</tbody>
</table>

Systems
**redistribute**

**Command Mode**  
Router Configuration (RIP or OSPF).

**Description**  
Creates an IP redistribute list entry.

IP redistribute list entries control the distribution of static, local, or dynamically learned routes from one protocol to another protocol. Route redistribution is supported only by dynamic routing protocols, such as RIP and OSPF.

* **Note:** Selecting OSPF as the destination protocol causes OSPF adjacencies to be reestablished. During this reestablishment, a temporary loss of traffic occurs.

**Syntax**

| To Redistribute Routes to RIP:                  | redistribute {ospf | local | static} [access-list-name] |
|------------------------------------------------|----------------------------------------------------------|
|                                                 | * **Note:** You must be in RIP Router Configuration mode to enter this command. |

| To Redistribute Routes to OSPF:               | redistribute {rip | local | static} [access-list-name] |
|------------------------------------------------|----------------------------------------------------------|
|                                                 | * **Note:** You must be in OSPF Router Configuration mode to enter this command. |

| To Delete an Entry that Redistributes Routes to RIP: | no redistribute {ospf | local | static} |
|------------------------------------------------------|------------------------------------------------|
|                                                     | * **Note:** You must be in RIP Router Configuration mode to enter this command. |

| To Delete an Entry that Redistributes Routes to OSPF: | no redistribute {rip | local | static} |
|-------------------------------------------------------|------------------------------------------------|
|                                                      | * **Note:** You must be in OSPF Router Configuration mode to enter this command. |
### Table 11-28. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospf</td>
<td>Redistributes OSPF routes to RIP. You must be in RIP Router Configuration mode to enter this keyword.</td>
</tr>
<tr>
<td>rip</td>
<td>Redistributes RIP routes to OSPF. You must be in OSPF Router Configuration mode to enter this keyword.</td>
</tr>
<tr>
<td>local</td>
<td>Redistributes local routes.</td>
</tr>
<tr>
<td>static</td>
<td>Redistributes static routes.</td>
</tr>
<tr>
<td>[&lt;access-list-name&gt;]</td>
<td>The access list that controls which routes are redistributed. Use this option if you want to redistribute only specific routes. The access list can either permit or deny specific routes for redistribution. If you do not enter this option, all routes are redistributed. <strong>Note:</strong> Avaya recommends that you do not globally enable an access list that you use to redistribute specific routes. <strong>Note:</strong> Route redistribution supports only standard access rules. You cannot use extended access rules to permit or deny specific routes for redistribution.</td>
</tr>
</tbody>
</table>
show arp

Command Mode  User.

Description  Displays the ARP cache.

Syntax  show arp [<ip-addr>] [<if-name>] [static]

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address for which you want to view the ARP entry.</td>
</tr>
<tr>
<td>&lt;if-name&gt;</td>
<td>The interface for which you want to view ARP entries.</td>
</tr>
<tr>
<td>[static]</td>
<td>Displays only static ARP entries.</td>
</tr>
</tbody>
</table>

Sample Output  The following example displays the ARP cache entry for IP address 122.100.0.17.

> show arp 122.100.0.17

<table>
<thead>
<tr>
<th>Address</th>
<th>MAC Address</th>
<th>I/F</th>
<th>Type</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>122.100.0.17</td>
<td>ff:ff:ff:ff:ff:ff</td>
<td>mgmt</td>
<td>Local</td>
<td>Not Aged</td>
</tr>
</tbody>
</table>

show hosts

**Command Mode**  
User.

**Description**  
Displays DNS Client information.

**Syntax**  
show hosts

**Sample Output**  
The following command displays the DNS Client information.

> show hosts

**Systems**  
show ip arp

Command Mode
User.

Description
Displays the Address Resolution Protocol (ARP) cache.

Syntax
show ip arp [<ip-addr>] [<if-name>] [static]

Sample Output
The following example displays the ARP cache entry for IP address 122.100.0.17.

> show ip arp 122.100.0.17

<table>
<thead>
<tr>
<th>Address</th>
<th>MAC Address</th>
<th>I/F</th>
<th>Type</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>122.100.0.17</td>
<td>ff:f:f:ff:ff:ff</td>
<td>mgmt</td>
<td>Local</td>
<td>Not Aged</td>
</tr>
</tbody>
</table>

Systems
show ip interface

Command Mode User.

Description Displays configuration information for the IP interface.

Syntax show ip interface [interface-name]

Sample Output The following command displays information for the interface labeled “boston”.

> show ip interface boston
boston is up, and administratively up
 On Ethernet Console, is up
 Internet address is 192.168.0.115, subnet mask is 255.255.255.0
 MTU is 1500 bytes
 Proxy ARP is enabled
 ICMP redirects are not sent

show ip irdp

Command Mode
User.

Description
Displays ICMP Router Discovery Protocol (IRDP) configuration.

Syntax
show ip irdp [ <interface-name> ]

Table 11-32. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-name&gt;</td>
<td>Interface-name is an optional argument. If specified, it requests ICMP IRDP information for the specified interface.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays the IRDP configuration on the switch.

> show ip irdp
Router# show ip irdp
Console has ICMP Router Discovery Protocol enabled.
   Network address is 192.168.60.53, subnet mask is 255.255.255.0
   Advertisements sent using Multicast.
   Advertisements occur between every 450 and 600 seconds
   Advertisements valid for 1800 seconds.
   Preference set to 0.
ip_if1 has ICMP Router Discovery Protocol disabled.
   Network address is 10.1.1.10, subnet mask is 255.255.255.0
   Advertisements sent using Multicast.
   Advertisements occur between every 450 and 600 seconds
   Advertisements valid for 1800 seconds.
   Preference set to 0

Systems
show ip redistribute

**Command Mode**  
User.

**Description**  
Displays IP redistribute list entries.

**Syntax**  
show ip redistribute

**Sample Output**  
redistribute ospf route into rip  
redistribute static route into rip  
redistribute local route into rip using access-list 1

**Systems**  
P580 and P882.
**show ip route**

**Command Mode** User

**Description** Displays information about the IP unicast routing table.

**Syntax**

```
show ip route [{rip | ospf | local | unknown | static}] [<ip-addr>] [<if-name>]
```

**Sample Output**

The following example displays the IP Route static information on the switch.

```
> show ip route static
0.0.0.0 0.0.0.0 via 192.168.0.1 cost=1
pref=low
```

**Systems**


---

**Table 11-33. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>rip</td>
<td>Displays all RIP routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>Displays all OSPF routes.</td>
</tr>
<tr>
<td>local</td>
<td>Displays all local IP interfaces.</td>
</tr>
<tr>
<td>unknown</td>
<td>Displays all unknown routes.</td>
</tr>
<tr>
<td>static</td>
<td>Displays all static routes.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>Displays routing information about the specified IP address.</td>
</tr>
<tr>
<td>&lt;if-name&gt;</td>
<td>Displays IP information about the interface.</td>
</tr>
</tbody>
</table>
show ip route summary

Command Mode User.

Description Displays a summary of the routing table.

Syntax show ip route summary

Sample Output IP Route Summary:
   Current number of routes: 3
   Peak number of routes : 3
   Total routes added : 4
   Total routes deleted : 1
   RIP route changes : 0
   RIP queries : 0

show ip short-lived

Command Mode     Global Configuration
Description      Displays the short-lived IP protocol filters that are currently enabled.
Syntax           show ip short-lived
Sample Output    After you enter the show ip short-lived command, the switch displays the filters that are currently enabled. For example:

    ip short-lived tcp 112
    ip short-lived udp 53
    ip short-lived udp 123

Systems          P580 and P882.
show ip traffic

Command Mode
User.

Description
Displays IP traffic statistics information.

Syntax
show ip traffic

Sample Output
The following example displays the IP traffic statistics information.

> show ip traffic
IP statistics:
  Received:
    115972 total, 15153 local destination
    0 packet header errors, 0 unknown protocol
    0 with address errors, 0 discarded
    Device is a gateway
  Fragments:
    0 reassembled, 0 couldn’t reassemble
    0 fragmented, 0 couldn’t fragment
  Sent:
    5132 generated, 0 forwarded
    0 no route, 0 discarded

ICMP statistics:
  Received:
    10 total, 0 ICMP errors, 0 unreachable
    0 time exceeded, 0 parameter, 0 quench
    0 redirects, 5 echo, 5 echo reply
    0 timestamp request, 0 timestamp reply
    0 mask requests, 0 mask replies
  Sent:
    10 total, 0 ICMP errors, 0 unreachable
    0 time exceeded, 0 parameter, 0 quench
    0 redirects, 5 echo, 5 echo reply
    0 timestamp request, 0 timestamp reply
    0 mask requests, 0 mask replies

UDP statistics:
  Received:
    10666 total, 0 errors, 0 no port
  Sent:
    0 total

TCP statistics:
  Received:
    4487 total, 0 errors
  Sent:
    4937 total

Systems
show tcp configuration

Command Mode User.

Description Displays the current TCP port settings for Telnet and HTTP.

Syntax show tcp configuration

Sample Output The following example displays the current TCP port settings for Telnet and HTTP:

`> show tcp configuration
Telnet port: 9998
HTTP port: 9999`

show tcp connections

Command Mode
User.

Description
Displays a list of open TCP connections.

Syntax
show tcp connections

Systems
show tcp statistics

Command Mode User.

Description Displays TCP connection statistics.

Syntax show tcp statistics

Sample Output TCP statistics
Retransmit timeout algorithm : vanj
Retransmit timeout minimum : 0 (milliseconds)
Retransmit timeout maximum : 240000 (milliseconds)
Maximum num of connections : 150
Number of Active opens : 0
Number of Passive opens : 376
Attempted connection fails : 3
Estab. connection resets : 0
Established connections : 1
Segments received : 5081
Segments sent : 5546
Segments retransmitted : 214
Inactivity period : 900 (seconds)

show udp statistics

Command Mode User.

Description Displays UDP connection statistics.

Syntax `show udp statistics`

Sample Output

```
UDP statistics
  Total datagrams received : 10722
  Datagrams without ports  : 0
  Datagrams in error      : 0
  Total Datagrams sent    : 0
```

Overview

This chapter describes the following commands:

- default-metric
- ip rip authentication key
- ip rip authentication mode
- ip rip default-route-mode
- ip rip poison-reverse
- ip rip receive version
- ip rip send version
- ip rip send-receive-mode
- network
- output-delay
- router rip
- show ip rip statistics
- timers basic
- triggered updates
default-metric

**Command Mode**  Interface Configuration.

**Description**  Sets the default RIP route metric. The no form of this command restores the default value. The default setting is 1.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>default-metric &lt;metric&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no default-metric</td>
</tr>
</tbody>
</table>

**Table 12-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;metric&gt;</td>
<td>The default RIP route metric value. The range is 0 to 15. The default setting is 1.</td>
</tr>
</tbody>
</table>

**Sample Output**  The following example sets the default RIP metric value on the interface labeled “boston” to 10.

```
(config-if:boston)# default-metric 10
```

ip rip authentication key

Command Mode  Interface Configuration.

Description  Sets the authentication password used on the interface. The no form of this command clears the password.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip rip authentication key &lt;password&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Clear:</td>
<td>no ip rip authentication key</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the authentication string used on interface labeled “boston” as abc.

```
(config-if:boston)# ip rip authentication key abc
```


Table 12-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;password&gt;</td>
<td>The authentication password for the interface. You can use up to 16 characters.</td>
</tr>
</tbody>
</table>
ip rip authentication mode

Command Mode
Interface Configuration.

Description
Specifies the type of authentication mode used in RIP Version 2 packets. Use the no form of this command to restore the default value of none.

Syntax

| To Configure: | ip rip authentication mode {simple | md5 | none} |
|---------------|-----------------------------------------------|
| To Restore Default: | no ip rip authentication mode |

Table 12-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| {simple | md5 | none} | The authentication type used in RIP Version 2 packets. Types include:  
| | • **simple** - clear text authentication.  
| | • **md5** - keyed MD5 authentication.  
| | • **none** - No authentication. |

Sample Output
The following example specifies md5 the type of authentication mode to use for interface labeled “boston”.

```
(config-if:boston)# ip rip authentication mode md5
```

Systems
ip rip default-route-mode

Command Mode
Interface Configuration.

Description
Sets the RIP default route characteristics. The no form of this command disables the default route characteristics.

Syntax

| To Configure: | ip rip default-route-mode {talk-only | listen-only | talk-listen | disable} |
|----------------|------------------------------------------------------------------|
| To Restore Default: | no ip rip default-route-mode |

Table 12-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| {talk-only|listen-only|talk-listen|disable} | The RIP default route characteristics.  
  - **talk-only** - The default route is advertised in RIP updates but ignored on incoming neighbor updates.  
  - **listen-only** - The default route is suppressed from RIP updates but accepted on incoming neighbor updates.  
  - **talk-listen** - The default route is advertised and accepted.  
  - **disable** - The default route is not advertised or accepted. |

Sample Output
The following example sets the RIP default route characteristics for interface labeled “boston” to talk-listen mode.

(config-if:boston)# ip rip default-route-mode talk-listen

Systems
**ip rip poison-reverse**

**Command Mode** Interface Configuration.

**Description** Enables split-horizon with poison reverse on an interface. The no form of this command disables the poison-reverse mechanism. The default state is split-horizon with poison reverse.

The split-horizon technique prevents information about routes from exiting the router interface through which the information was learned. This prevents routing loops.

Poison reverse updates explicitly indicate that a network or subnet is unreachable rather than implying they are not reachable. Poison reverse updates are sent to defeat large routing loops.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip rip poison-reverse</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip rip poison-reverse</td>
</tr>
</tbody>
</table>

**Sample Output** The following example enables split-horizon with poison reverse on interface labeled “boston”.

```
(config-if:boston)# ip rip poison-reverse
```

**ip rip receive version**

**Command Mode**
Interface Configuration.

**Description**
Specifies a RIP version to receive on an interface basis. Use the no form of this command to restore the default setting of RIP Version 1.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip rip receive version [1] [2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip rip receive version</td>
</tr>
</tbody>
</table>

**Table 12-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| [1] [2] | The version of the RIP packets received on an interface.  
  • 1 - accept RIP Version 1 packets.  
  • 2 - accept RIP Version 2 packets. |

**Sample Output**
The following example specifies that the interface labeled “boston” receive RIP version 2 packets.

```
(config-if:boston)# ip rip receive version 2
```

**Systems**
ip rip send version

**Command Mode**  Interface Configuration.

**Description**  Specifies a RIP version to send on an interface basis. Use the no form of this command to restore the default setting of RIP Version 1.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip rip send version [1] [2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no ip rip send version</td>
</tr>
</tbody>
</table>

**Table 12-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1] [2]</td>
<td>The version of the RIP packets sent out the interface.</td>
</tr>
<tr>
<td></td>
<td>• 1 - send RIP Version 1 packets.</td>
</tr>
<tr>
<td></td>
<td>• 2 - send RIP Version 2 packets</td>
</tr>
</tbody>
</table>

**Sample Output**  The following specifies that the interface labeled “boston” send RIP version 2 packets.

```
(config-if:boston)# ip rip send version 2
```

**ip rip send-receive-mode**

**Command Mode**

Interface Configuration.

**Description**

Sets the RIP Send and Receive mode on an interface. The default state is talk-listen.

**Syntax**

ip rip send-receive-mode {talk-only | listen-only | talk-listen}

**Table 12-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{talk-only</td>
<td>listen-only</td>
</tr>
<tr>
<td></td>
<td>• <strong>talk-only</strong> - Set RIP to only transmit updates on the interface and not receive them.</td>
</tr>
<tr>
<td></td>
<td>• <strong>listen-only</strong> - set RIP to only receive updates on the interface and not transmit them.</td>
</tr>
<tr>
<td></td>
<td>• <strong>talk-listen</strong> - set RIP to transmit and receive updates on the interface.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example sets rip send-receive mode on the interface labeled “boston” to listen-only.

```
(config-if:boston)# ip rip send-receive-mode listen-only
```

**Systems**

network

Command Mode
RIP Router Configuration.

Description
Enables RIP routing on a network or networks. The no form of this command disables RIP routing.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>network &lt;ip-addr&gt; [&lt;wildcard-mask&gt;]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no network &lt;ip-addr&gt; [&lt;wildcard-mask&gt;]</td>
</tr>
</tbody>
</table>

Sample Output
The following example enables RIP on the 11.0.0.0 subnet which is connected to the 11.0.4.5 interface:

(configure router:rip)# network 11.0.4.5 255.255.255.255

Systems
output-delay

**Command Mode**  
RIP Router Configuration.

**Description**  
Specifies the interpacket delay for RIP updates. The **no** form of this command removes a delay definition. The default delay time is 1 second.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>output-delay &lt;delay&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no output-delay</td>
</tr>
</tbody>
</table>

**Table 12-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;delay&gt;</td>
<td>The delay between packets in a multiple-packet RIP update. The range is 0 to 50 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the interpacket delay for RIP updates to 10 seconds.

```
(configure router:rip)# output-delay 10
```

**Systems**  
router rip

Command Mode  Global Configuration.

Description  Globally enables or disables RIP. The no form of the command disables RIP. The default state is Enabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>router rip</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no router rip</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables RIP on the switch.

```
(configure) # router rip
```

timers basic

Command Mode  RIP Router Configuration.

Description  Adjusts RIP network timers. The no form of this command restores the default timers. The default for the update timer is 30 seconds, and the invalid time default is 120 seconds.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>timers basic &lt;update&gt; &lt;invalid&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no timers basic</td>
</tr>
</tbody>
</table>

Table 12-10. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;update&gt;</td>
<td>Rate, in seconds, updates are sent. This is the fundamental timing parameter of the routing protocol. The valid range is 10 to 50 seconds. The default setting is 30 seconds.</td>
</tr>
<tr>
<td>&lt;invalid&gt;</td>
<td>Interval of time, in seconds, after which a route is declared invalid. This value should be at least three times the value of update. The valid range is 1 to 65,535 seconds. The default setting is 120 seconds. A route becomes invalid when there is an absence of updates that refresh the route. The route then enters holddown. The route is marked inaccessible and advertised as unreachable. However, the route is still used for forwarding packets.</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the update value to 60 seconds.

(configure router:rip) # timers basic 60 120

triggered updates

Command Mode  
RIP Router Configuration.

Description  
Globally enables the use of RIP triggered updates. The no form of this command globally disables RIP triggered updates. The default state is disabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>triggered updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no triggered updates</td>
</tr>
</tbody>
</table>

Sample Output  
The following example globally enables the triggered updates function.

```
(configure router:rip)# triggered updates
```

Systems  
### show ip rip statistics

<table>
<thead>
<tr>
<th><strong>Command Mode</strong></th>
<th>User.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Displays RIP interface statistics.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show ip rip statistics</code></td>
</tr>
<tr>
<td><strong>Sample Output</strong></td>
<td>The following example displays IP interface statistics on interface 3.</td>
</tr>
</tbody>
</table>

```plaintext
> show ip rip statistics
intf3 10.0.3.45
State is DOWN
Triggered Updates Sent0
Un-triggered Updates Sent0
Updates Received0
Bad Packets Received0
Bad Routes Received0
```

Overview

This chapter describes the following commands:

- clear ipx route
- clear ipx service
- ipx advertise-default-route-only
- ipx default-route
- ipx delay
- ipx down
- ipx gns-reply-disable
- ipx gns-response-delay
- ipx network
- ipx output-rip-delay
- ipx output-sap-delay
- ipx rip
- ipx rip-filter
- ipx rip-max-packetsize
- ipx rip-multiplier
- ipx route
- ipx router
- ipx routing
- ipx sap
- ipx sap-max-packetsize
- ipx sap-multiplier
- ipx sap-name-filter
- ipx sap-network-filter
- ipx send-receive-mode
- ipx send-triggered-updates
- ipx service
- ipx type-20-propagation
- ipx update interval
- ipx vlan
- show ipx cache
- show ipx interface
- show ipx rip statistics
- show ipx rip-filter
- show ipx route
- show ipx sap statistics
- show ipx sap-name-filter
- show ipx sap-network-filter
- show ipx service
- show ipx traffic
clear ipx route

Command Mode Global Configuration.

Description Deletes routes from the IPX routing table. This command only deletes routes learned via the RIP routing protocol. Static and local routes cannot be deleted using this command.

Syntax clear ipx route \{<network> | default | *\}

Table 13-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{network</td>
<td>default</td>
</tr>
<tr>
<td>*</td>
<td>- Deletes all routes in the routing table.</td>
</tr>
<tr>
<td>default</td>
<td>- deletes the default route from the routing table.</td>
</tr>
<tr>
<td>network</td>
<td>- The number of the network whose routing table entry you want to display. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.</td>
</tr>
</tbody>
</table>

Sample Output The following example clears the entry for network 5 from the IPX routing table.

(configure)# clear ipx route 5

### clear ipx service

**Command Mode**
Global Configuration.

**Description**
Deletes services from the IPX service table. This command only deletes services learned via the SAP protocol. Static services cannot be deleted using this command.

**Syntax**
clear ipx service {<service-type> <service-name> | *}

### Table 13-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{&lt;service-type&gt; &lt;service-name&gt;</td>
<td>*}</td>
</tr>
<tr>
<td></td>
<td>- service-type - The type number of the service. The range is 0-FFFF.</td>
</tr>
<tr>
<td></td>
<td>- service-name - The name of the service - the length is 1 to 47 bytes.</td>
</tr>
<tr>
<td></td>
<td>- * - Deletes all services from the routing table.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example deletes all SAP-learned services in the IPX routing table.

```
(configure) # clear ipx service *
```

**Systems**
ipx advertise-default-route-only

Command Mode
Interface Configuration.

Description
Advertises only the default RIP route. The no form of this command advertises all known routes out the interface.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx advertise-default-route-only</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx advertise-default-route-only</td>
</tr>
</tbody>
</table>

Sample Output
The following example advertises only the default RIP route configured on an interface labeled “boston”.

(config-if:boston)# ipx advertise-default-route-only

Systems
ipx default-route

**Command Mode**
Global Configuration.

**Description**
Forwards all packets for which a route to the destination network is unknown, to the default network. The no form of this command restores the default state which disables use of the default network.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx default-route</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx default-route</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example forwards all packets to the ipx default route if the route is unknown:

```
(configure)# ipx default-route
```

**Systems**
**ipx delay**

**Command Mode**  Interface Configuration.

**Description**  Sets the ticks for an IPX interface. The no form of this command restores the system default, which is 1 tick.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ipx delay &lt;ticks&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ipx delay</td>
</tr>
</tbody>
</table>

**Table 13-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ticks&gt;</td>
<td>Number of IBM clock ticks of delay to use. One clock tick is 55 milliseconds (1/18th of a second). The range is 1 to 32000 ticks.</td>
</tr>
</tbody>
</table>

**Sample Output**  The following example sets the ticks for the interface labeled “boston” to 20000.

```
(config-if:boston)# ipx delay 20000
```

### ipx down

**Command Mode**
Interface Configuration.

**Description**
Administratively shuts down an IPX network. The no form restarts the network. The default state is disable, which means IPX is not shut down.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx down</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx down</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example shuts down the IPX network on the interface labeled “boston”.

```
(config-if:boston)# ipx down
```

**Systems**
**ipx gns-reply-disable**

**Command Mode** Interface Configuration.

**Description** Disables the sending of replies to IPX Get Nearest Server (GNS) queries. The no form restores the default state of enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx gns-reply-disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx gns-reply-disable</td>
</tr>
</tbody>
</table>

**Sample Output** The following example disables the sending of replies to the IPX GNS on an interface labeled “boston”.

```
(config-if:boston)# ipx gns-reply-disable
```

Chapter 13

### ipx gns-response-delay

**Command Mode**  
Interface Configuration.

**Description**  
Sets the delay time (milliseconds) when responding to IPX GNS requests. The no form of this command restores the default. The default is zero, which indicates no delay.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ipx gns-response-delay &lt;milliseconds&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ipx gns-response-delay</td>
</tr>
</tbody>
</table>

**Table 13-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;milliseconds&gt;</td>
<td>The time, in milliseconds, that the switch waits after receiving a GNS request from an IPX client before responding with a server name to that client. The range is 0 to 5000 milliseconds.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example sets the delay time for an interface labeled “boston” to respond to IPX GNS requests to 200 milliseconds.

```
(config-if:boston) # ipx gns-response-delay 200
```

**Systems**

ipx network

**Command Mode**
Interface Configuration.

**Description**
Enable IPX on a particular interface and select the network number and type of encapsulation (optional). The no form of this command disables IPX routing. The IPX routing default is disabled, and the default encapsulation type is arpa.

**Syntax**

| To Configure: | ipx network <network> [encapsulation {arpa | novell-ether | sap | snap}] |
|---------------|---------------------------------------------------------------|
| To Disable:   | [no] ipx network <network>                                   |

**Table 13-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;network&gt;</td>
<td>The IPX network address. This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. The range is 1 to FFFFFFFD.</td>
</tr>
<tr>
<td>encapsulation</td>
<td>The encapsulation (framing) type. Options are:</td>
</tr>
<tr>
<td>{arp</td>
<td>novell-ether</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>novell-ether</strong> - Use Novell's “Ethernet_802.3” encapsulation. This encapsulation consists of a standard 802.3 Media Access Control (MAC) header followed directly by the IPX header with a checksum of FFFF. It is the default encapsulation used by all versions of NetWare up to and including Version 3.11.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>sap</strong> - Use Novell's Ethernet_802.2 encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 LLC header. This is the default encapsulation used by NetWare Version 3.12 and 4.0.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>snap</strong> - Use Novell Ethernet_Snap encapsulation. This encapsulation consists of a standard 802.3 MAC header followed by an 802.2 SNAP LLC header.</td>
</tr>
</tbody>
</table>
Sample Output The following example enables IPX routing on network 2 on an interface labeled “boston” and sets encapsulation to SNAP.

(config-if:boston)# ipx network 2 encapsulation snap

ipx output-rip-delay

Command Mode  Interface Configuration.

Description  Sets the interpacket delay for RIP updates sent on a single interface. The no form of this command results in no interpacket delay. The default state is enabled, which is a 55-millisecond delay.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx output-rip-delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx output-rip-delay</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables the interpacket delay for IPX output RIP updates sent out on an interface labeled “boston”.

```
(config-if:boston)# ipx output-rip-delay
```

**ipx output-sap-delay**

**Command Mode**
Interface Configuration.

**Description**
Sets the interpacket delay for Service Advertising Protocol (SAP) updates sent on a single interface. The no form of this command results in no interpacket delay. The default state is enabled, which is a 55 millisecond delay.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx output-sap-delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx output-sap-delay</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the interpacket delay for SAP on an interface labeled “boston”.

```
(config-if:boston)# ipx output-sap-delay
```

**Systems**
**ipx rip**

**Command Mode**
Interface Configuration.

**Description**
Enables IPX RIP on an interface. The no form of this command disables IPX RIP on the interface. The default interface setting is IPX RIP enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable</th>
<th>ipx rip</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable</td>
<td>[no] ipx rip</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables IPX RIP on an interface labeled “boston”.

```
(config-if:boston)# ipx rip
```

**Systems**
**ipx rip-filter**

**Command Mode**
Interface Configuration.

**Description**
Controls which networks are present in RIP packets sent and received on the interface. The no form of this command removes the filter from an interface.

**Syntax**

| To Configure: | ipx rip-filter <precedence> <start-network> <end-network> [outbound | inbound | both] {filter | allow} [<filter-ticks> [<filter-hops>]] |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|
| To Remove:    | [no] ipx rip-filter <precedence>                                                                                                  |

**Table 13-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;precedence&gt;</td>
<td>Indicates the precedence of this RIP filter in relation to other RIP filters on this interface. Lower numbers indicate a higher precedence. The range is 0-9999.</td>
</tr>
<tr>
<td>&lt;start-network&gt;</td>
<td>The first IPX network address this filter should match. The range is 0-FFFFFFF.</td>
</tr>
<tr>
<td>&lt;end-network&gt;</td>
<td>The last IPX network address this filter should match. The range is 0-FFFFFFF.</td>
</tr>
</tbody>
</table>
| {outbound | inbound | both} | The filter direction.  
  - **outbound** - apply filter to RIP packets sent out the interface.  
  - **inbound** - apply filter to RIP packets received on the interface.  
  - **both** - apply filter to RIP packets in both directions. |
| {filter | allow} | The action to take for the IPX network in question.  
  - **filter** - do not add the network to the routing table (inbound RIP packets) or do not advertise the network (outbound RIP packets).  
  - **allow** - add the network to the routing table (inbound RIP packets) or advertise the network (outbound RIP packets). |
Sample Output

The following example:

- sets the IPX RIP filter precedence to 5
- sets the start-network to 2
- sets the end-network to 3
- applies filters to RIP packets in both directions (both)
- adds the network to the routing table (allow)
- sets the filter ticks to 10000
- sets the filter hops to 5

on an interface labeled “boston”.

(config-if:boston)# ipx rip-filter 5 2 3 both allow 10000 5

Systems


<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filter-ticks&gt;</td>
<td>Modify the number of ticks to get to the network in the routing table (inbound RIP packets) or in the advertised information (outbound RIP packets). The range is 0 to 32000 ticks.</td>
</tr>
<tr>
<td>&lt;filter-hops&gt;</td>
<td>Modify the number of hops to get to the network in the routing table (inbound RIP packets) or in the advertised information (outbound RIP packets). The range is 0 to 16 hops.</td>
</tr>
</tbody>
</table>
**ipx rip-max-packetsize**

**Command Mode**  
Interface Configuration.

**Description**  
Enables the maximum packet size for RIP updates sent out the interface. To restore the default packet size, use the no form of this command. The default state is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx rip-max-packetsize</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx rip-max-packetsize</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example enables the maximum packet size for RIP updates on an interface labeled “boston”.

```
(config-if:boston)# ipx rip-max-packetsize
```

**Systems**  
ipx rip-multiplier

Command Mode
Interface Configuration.

Description
Sets the interval at which a network’s RIP entry ages out. The no form of this command restores the default. The default value is three times the RIP update interval.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ipx rip-multiplier &lt;multiplier&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ipx rip-multiplier</td>
</tr>
</tbody>
</table>

Table 13-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;multiplier&gt;</td>
<td>The multiplier used to calculate the interval at which RIP routing table entries age out. This can be any positive number. The value you specify is multiplied by the RIP update interval to determine the aging-out interval.</td>
</tr>
</tbody>
</table>

Sample Output
The following example sets the IPX RIP age-out interval on an interface labeled “boston” to 40.

(config-if:boston)# ipx rip-multiplier 40

Systems
ipx route

Command Mode

Global Configuration.

Description

Adds a static route to the routing table. The no form of this command removes a route from the routing table.

Syntax

To Configure:  
```
ipx route { <network> | default } <network.next-hop-node> [ <ticks> [ <hops> ] ]
```

To Remove:  
```
[ no ] ipx route { <network> | default } <network.next-hop-node>
```

Table 13-8. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| { network | default }                  | • network - an eight-digit hexadecimal number that identifies the network on which you are establishing a static route.  
                              |     The range is 1 to FFFFFFFFD and leading zeros can be omitted (for 000000BB, enter BB).  
                              |     • default - creates a static entry for the default-route. |
| <network.next-hop-node>       | Network number and node address of the next hop to the server.  
                              |     • next-hop-node - The argument node is the node number of the target Novell server. This is a 48-bit value represented by a MAC address (aa:bb:cc:dd:ee:ff). |
| <ticks>                       | Number of IBM clock ticks of delay to the network for which you are establishing a static route. The range is 1 to 32000. |
| <hops>                        | Number of hops to the network for which you are establishing a static route. The range is 1 to 16. |

Sample Output

The following example adds a static route to the routing table.

```
(configure) # ipx route 50 100:02:e0:3b:00:45:63
```

Systems

ipx router

Command Mode  Global Configuration.

Description  Enables the IPX RIP or IPX SAP protocol on a global basis. Use the no form of the command to disable the protocols. The default state is enabled.

Syntax

| To Enable:               | ipx router {rip | sap} |
|-------------------------|------------------------|
| To Disable:             | [no] ipx router {rip | sap} |

Table 13-9. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{rip</td>
<td>sap}</td>
</tr>
</tbody>
</table>

Sample Output  The following example disables IPX RIP on a global basis.

(configure)# no ipx router rip

### ipx routing

**Command Mode**
Global Configuration.

**Description**
Enables IPX routing. The no form of this command disables IPX routing. The default state is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ipx routing</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables IPX routing.

```
(configure) # ipx routing
```

**Systems**
ipx sap

**Command Mode** Interface Configuration.

**Description** Enables IPX SAP on an interface. The no form of this command disables IPX SAP on an interface. Default interface setting is IPX SAP enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx sap</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx sap</td>
</tr>
</tbody>
</table>

**Sample Output** The following example disables IPX SAP on an interface labeled “boston”.

```bash
(config-if:boston)# no ipx sap
```

**ipx sap-max-packetsize**

**Command Mode**
Interface Configuration.

**Description**
Enables use of the maximum packet size for SAP updates sent out the interface. The no form of this command disables this function. The default state is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx sap-max-packetsize</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx sap-max-packetsize</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables use of the maximum packet size for SAP updates sent out the *boston* interface.

```plaintext
(config-if:boston)# ipx sap-max-packetsize
```

**Systems**
**ipx sap-multiplier**

**Command Mode**
Interface Configuration.

**Description**
Sets the interval at which a network or server’s SAP entry ages out. The no form of this command restores the default, which is three times the SAP update interval.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ipx sap-multiplier &lt;multiplier&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ipx sap-multiplier</td>
</tr>
</tbody>
</table>

**Table 13-10. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| <multiplier> | The multiplier used to calculate the interval SAP routing table entries age out. This can be any positive number.  
  The value you specify is multiplied by the SAP update interval to determine the aging-out interval. |

**Sample Output**
The following example sets the interval at which the SAP entry goes out to 20 on an interface labeled “boston”.

```
(config-if:boston)# ipx sap-multiplier 20
```

**Systems**
**ipx sap-name-filter**

**Command Mode**  
Interface Configuration.

**Description**  
Specifies which services (by name) are present in SAP packets sent and received on the interface. The no form of this command removes a filter from the interface.

**Syntax**

| To Configure: | ipx sap-name-filter <precedence> <filter-name> <service-type> {outbound | inbound | both} {filter | allow} [<filter-hops>] |
|---------------|---------------------------------------------------------------------------------------------------------------------------|
| To Remove:    | [no] ipx sap-name-filter <precedence> |

**Table 13-11. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;precedence&gt;</td>
<td>Indicates the precedence of this SAP name filter in relation to other SAP name filters on this interface. Lower numbers indicate a higher precedence. The range is 0-9999.</td>
</tr>
<tr>
<td>&lt;filter-name&gt;</td>
<td>The name of the service that this filter matches. The filter-name is compared against the Service name for a match. A single asterisk may be present as the last character of filter-name, which matches all remaining characters. Up to 1 to 63 bytes are allowed.</td>
</tr>
<tr>
<td>&lt;service-type&gt;</td>
<td>The IPX service type (hexadecimal). This is between 0 and FFFF, where FFFF matches all service types.</td>
</tr>
<tr>
<td>{outbound</td>
<td>inbound</td>
</tr>
<tr>
<td></td>
<td>• outbound - Apply filter to SAP packets sent out the interface.</td>
</tr>
<tr>
<td></td>
<td>• inbound - Apply filter to SAP packets received on the interface.</td>
</tr>
<tr>
<td></td>
<td>• both - Apply filter to SAP packets in both directions.</td>
</tr>
</tbody>
</table>
Table 13-11. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>(filter</td>
<td>allow)</td>
</tr>
<tr>
<td></td>
<td>• filter - Do not add the service to the service table (inbound SAP packets) or do not advertise the service (outbound SAP packets).</td>
</tr>
<tr>
<td></td>
<td>• allow - Add the service to the service table (inbound SAP packets) or advertise the service (outbound SAP packets).</td>
</tr>
<tr>
<td>&lt;filter-hops&gt;</td>
<td>The number of hops to get to the service in the service table (inbound SAP packets) or in the advertised information (outbound SAP packets). The range is 0 to 16 hops.</td>
</tr>
</tbody>
</table>

Sample Output

The following example:

- sets the precedence to 2
- sets the filter-name to netbios
- sets the service type to 1
- applies filters to SAP packets in both directions (both)
- adds the service to the service table (allow)
- sets the filter hops to 4

on an interface labeled “boston”.

(config-if:boston) # ipx sap-name-filter 2 netbios 1 both allow 4

Systems

ipx sap-network-filter

**Command Mode**
Interface Configuration.

**Description**
Specifies which services (by network) are present in SAP packets sent and received on the interface. The no form of this command removes the filter from an interface.

**Syntax**

| To Configure: | ipx sap-network-filter <precedence> <filter-network> <service-type> {outbound | inbound | both} {filter | allow} [ <filter-hops>] |
| To Remove:     | [no] ipx sap-network-filter <precedence> |

**Table 13-12. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;precedence&gt;</td>
<td>Indicates the precedence of this SAP name filter in relation to other SAP name filters on this interface. Lower numbers indicate a higher precedence. The range is 0-9999.</td>
</tr>
<tr>
<td>&lt;filter-network&gt;</td>
<td>The network of the service that this filter matches. The range is 0 - FFFFFFFF where, FFFFFFFF matches all networks.</td>
</tr>
<tr>
<td>&lt;service-type&gt;</td>
<td>The type of the IPX SAP service, in hexadecimal. The range is 0 - FFFF where, FFFF matches all service types.</td>
</tr>
<tr>
<td>{outbound</td>
<td>inbound</td>
</tr>
<tr>
<td></td>
<td>• outbound - Apply filter to SAP packets sent out the interface.</td>
</tr>
<tr>
<td></td>
<td>• inbound - Apply filter to SAP packets received on the interface.</td>
</tr>
<tr>
<td></td>
<td>• both - Apply filter to SAP packets in both directions.</td>
</tr>
</tbody>
</table>
Table 13-12. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{filter</td>
<td>allow}</td>
</tr>
<tr>
<td></td>
<td>• filter - Do not add the service to the service table (inbound SAP packets) or do not advertise the service (outbound SAP packets).</td>
</tr>
<tr>
<td></td>
<td>• allow - Add the service to the service table (inbound SAP packets) or advertise the service (outbound SAP packets).</td>
</tr>
<tr>
<td>&lt;filter-hops&gt;</td>
<td>The number of hops to get to the service in the service table (inbound SAP packets) or in the advertised information (outbound SAP packets). The range is 0 to 16 hops.</td>
</tr>
</tbody>
</table>

Sample Output

The following example:

- sets the SAP name filter precedence to 1
- sets the filter-network to 3
- sets the service-type to 2
- applies filters to SAP packets in both directions (both)
- adds the service to the service table (allow)
- sets the filter hops to 4

on an interface labeled “boston”.

(config-if:boston)# ipx sap-network-filter 1 3 2 both allow 4

Systems

ipx send-receive-mode

Command Mode Interface Configuration.

Description Sets the RIP/SAP send and receive characteristics of the IPX interface. The no form of this command restores the default, which is talk-listen.

Syntax

| To Configure:          | ipx send-receive-mode {rip | sap} {talk-only | listen-only | talk-listen} |
|------------------------|----------------------------------------------------------|
| To Restore Default:    | [no] ipx send-receive-mode {rip | sap}                  |

Table 13-13. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{rip</td>
<td>sap}</td>
</tr>
<tr>
<td>{talk-only</td>
<td>listen-only</td>
</tr>
<tr>
<td></td>
<td>• listen-only - RIP or SAP only receives updates on the interface and does not transmit them.</td>
</tr>
<tr>
<td></td>
<td>• talk-listen - RIP or SAP transmits and receives updates on the interface.</td>
</tr>
</tbody>
</table>

Sample Output The following example sets the RIP send-receive characteristics for an interface labeled “boston” to talk-listen.

(config-if:boston)# ipx send-receive-mode rip talk-listen

### ipx send-triggered-updates

**Command Mode** Interface Configuration.

**Description** Immediately sends RIP or SAP updates to the network in response to changes in the network topology. The no command disables triggered updates. The default setting is enabled.

**Syntax**

| To Enable:         | ipx send-triggered-updates {rip | sap} |
|--------------------|---------------------------------------|
| To Disable:        | [no] ipx send-triggered-updates {rip | sap} |

**Table 13-14. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{rip</td>
<td>sap}</td>
</tr>
</tbody>
</table>

ipx service

**Command Mode**
Global Configuration.

**Description**
Specifies static SAP entries. To remove static SAP entries, use the `no` form of this command. The default is that no static services are defined.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ipx service <code>&lt;service-type&gt;</code> <code>&lt;service-name&gt;</code> <code>&lt;network&gt;</code> <code>&lt;node&gt;</code> <code>&lt;socket&gt;</code> <code>&lt;network.next-hop-node&gt;</code> [ <code>&lt;hops&gt;</code> ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td><code>[no] ipx service </code>&lt;service-type&gt;<code> </code>&lt;service-name&gt;``</td>
</tr>
</tbody>
</table>

**Table 13-15. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;service-type&gt;</code></td>
<td>The number of the type of the service. The range is 0-FFFF.</td>
</tr>
<tr>
<td><code>&lt;service-name&gt;</code></td>
<td>Name of the server that provides the service. The range is 1 to 47 bytes long.</td>
</tr>
<tr>
<td><code>&lt;network&gt;</code></td>
<td>An eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFF. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA you can enter AA.</td>
</tr>
<tr>
<td><code>&lt;node&gt;</code></td>
<td>The node number of the target Novell server. This is a 48-bit value represented by a MAC address (aa:bb:cc:dd:ee:ff).</td>
</tr>
<tr>
<td><code>&lt;socket&gt;</code></td>
<td>The socket number for this service. The range is 0 - FFFF</td>
</tr>
<tr>
<td><code>&lt;network.next-hop-node&gt;</code></td>
<td>Network number and node address of the next hop to the server.</td>
</tr>
<tr>
<td><code>&lt;next-hop-node&gt;</code></td>
<td>The argument node is the node number of the target Novell server. This is a 48-bit value represented by a MAC address (aa:bb:cc:dd:ee:ff).</td>
</tr>
<tr>
<td><code>&lt;hops&gt;</code></td>
<td>Number of hops to the server. The range is 1-16.</td>
</tr>
</tbody>
</table>
The following example adds a static service to the service table.

```
(configure)# ipx service 4FS_ENG01 36112114 00:00:00:00:00:01 451 100.02:e0:3b:00:45:63
```

Systems

ipx type-20-propagation

Command Mode
Interface Configuration.

Description
Specifies whether or not an IPX interface accepts and forwards IPX type 20 propagation packet broadcasts. The default setting is disabled.

Syntax

| To Enable: | ipx type-20-propagation {both | inbound | outbound} |
|-----------|-----------------------------------------------------|
| To Disable: | ipx type-20-propagation disabled |

Table 13-16. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{both</td>
<td>inbound</td>
</tr>
<tr>
<td></td>
<td>• <strong>inbound</strong> - The interface only accepts type 20 broadcast packets.</td>
</tr>
<tr>
<td></td>
<td>• <strong>outbound</strong> - The interface only forwards type 20 propagation broadcast packets to other network segments.</td>
</tr>
<tr>
<td></td>
<td>• <strong>disabled</strong> - The interface does not accept or forward type 20 propagation broadcast packets.</td>
</tr>
</tbody>
</table>

Sample Output
The following example forwards type 20 propagation broadcast packets to other network segments on an interface labeled “boston”.

```
(config-if:boston)# ipx type-20-propagation outbound
```

Systems
ipx update interval

**Command Mode**  
 Interface Configuration.

**Description**  
 Adjusts the RIP or SAP update interval. The no form of this command restores the default, of 60 seconds.

**Syntax**

| To Configure: | ipx update interval {rip | sap} <seconds> |
|---------------|------------------------------------------|
| To Restore Default: | [no] ipx update interval |

**Table 13-17. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| {rip | sap}    | • rip - Adjusts the interval at which RIP updates are sent. The minimum interval is 10 seconds.  
|             | • sap - Adjusts the interval at which SAP updates are sent. The minimum interval is 10 seconds. |
| <seconds>    | The update interval. The range is 10 - 604800 seconds.                     |

**Sample Output**

The following example modifies the RIP update interval to 1000 seconds on an interface labeled “boston”.

```plaintext
(config-if:boston)# ipx update interval rip 1000
```

**Systems**

ipx vlan

**Command Mode**  Interface Configuration.

**Description**  Specifies the VLAN on which the IPX interface operates. The no form of this command assigns the IPX interface to the discard VLAN.

**Syntax**

| To Configure: | ipx vlan {<vlan-id> | name <vlan-name>} |
|---------------|-----------------------------------|
| To Disable:   | [no] ipx vlan                    |

**Table 13-18. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The VLAN ID of the VLAN.</td>
</tr>
<tr>
<td>name</td>
<td>&lt;vlan-name&gt; - The name of the VLAN</td>
</tr>
</tbody>
</table>

**Sample Output**  The following example specifies that the IPX on AN interface labeled “boston” reside on VLAN 200.

```
(config-if:boston)# ip vlan 200
```

show ipx cache

Command Mode
User.

Description
Displays the contents of the IPX fast-switching cache.

Syntax
show ipx cache

Sample Output
The following is an example of the output that displays after you enter the
display ipx cache command.

PRE 6
  Tree is IPX
  Access Rule is None
  Destination Address is 36112214
  Source Address is 0
  Destination Port is 0
  Source Port is 0
  Comp is DA
  TTL is 0
  Age is 0
  Filter is No
  Destination VLAN is tiny100
  Source VLAN is 00:c0:4f:ae:6b:6d
  Use is 1
  Priority is 0
  Format is Eth2
  .
  .
  .

Systems
show ipx interface

**Command Mode**  
User.

**Description**  
Displays the details of IPX interfaces configured on the switch.

**Syntax**  
show ipx interface [<intf-name>]

**Sample Output**  
The following is an example of the output that displays after you enter the `show ipx interface` command.

10005129 is up, and administratively up  
On vlan ipxServer, is up  
IPX address is 10005129.02:e0:3b:d4:48:03, encapsulation type Ethernet SNAP  
MTU is 1492 bytes  
Delay of this Novell network, in ticks, is 1  
IPX Type 20 propagation packet forwarding mode is set to Inbound  
IPX RIP is enabled on this interface  
IPX RIP periodic update packets have an interpacket gap of 55 msec  
IPX RIP updates are sent with up to 50 networks per packet  
Sending of IPX RIP triggered updates is enables  
IPX RIP update interval is 60 seconds  
IPX RIP aging interval multiplier is 3

**Systems**  
show ipx rip statistics

**Command Mode** User.

**Description** Displays the following IPX RIP interface statistics:

- Triggered Updates Sent
- Non-triggered Updates Sent
- Updates Received
- Requests Received
- Bad Packets Received

**Syntax** show ipx rip statistics

show ipx rip-filter

Command Mode    User.

Description    Displays IPX RIP filters.

Syntax    show ipx rip-filter

show ipx route

Command Mode  User.

Description  Displays the contents of the IPX Routing Table.

Syntax  show ipx route [{<network> | default}]

Sample Output  The following is an example of the output that displays after you enter the show ipx route command.

    Codes:  C - Connected primary network,  S - Static,  R - RIP
            s - seconds
    7 Total IPX routes.

    IPX default route known
    C 100  (Ethernet 802.3), 100
    C 1001 (Ethernet II), 1001
    C 1002 (Ethernet 802.2), 1002
    C 1003 (Ethernet SNAP), 1003
    C 10005129(Ethernet SNAP), 10005129
    R AAAAAAAA[2/2] via 10005129.00:c0:4f:ae:6b:6d, 10005129
    S FFFFFFFFvia 100.02:e0:3b:00:45:63, 100


Table 13-20. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;network&gt;</td>
<td>The number of the network whose routing table entry you want to display.  This is an eight-digit hexadecimal number that uniquely identifies a network cable segment. It can be a number in the range 1 to FFFFFFFD. You do not need to specify leading zeros in the network number. For example, for the network number 000000AA, you can enter AA.</td>
</tr>
<tr>
<td>default</td>
<td>Displays the default route. This is equivalent to specifying a value of FFFFFFFE for the argument network.</td>
</tr>
</tbody>
</table>
show ipx sap statistics

**Command Mode**

User.

Displays the following IPX SAP interface statistics:

- Triggered Updates Sent
- Non-triggered Updates Sent
- GNS Responses Sent
- Updates Received
- Requests Received
- GNS Requests Received
- Bad Packets Received

**Syntax**

show ipx sap statistics

**Systems**

**show ipx sap-name-filter**

**Command Mode**  
User.

**Description**  
Displays IPX SAP name filters.

**Syntax**  
show ipx sap-name-filter

**Systems**  
show ipx sap-network-filter

Command Mode  User.

Description  Displays IPX SAP network filters.

Syntax  show ipx sap-network-filter

show ipx service

Command Mode
User.

Description
Lists the IPX services added via static configuration or discovered through Service Advertising Protocol (SAP) advertisements.

Syntax
show ipx service

Sample Output
The following is an example of the output that displays after you enter the show ipx service command.

<table>
<thead>
<tr>
<th>Code</th>
<th>Type</th>
<th>Name</th>
<th>Address</th>
<th>Route Hops</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ifx</td>
<td></td>
<td>FileServer2</td>
<td>60.00:00:00:00:00:01.0455</td>
<td>0/0 1</td>
</tr>
<tr>
<td>S</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>4</td>
<td>SQA1</td>
<td>36112214.00:00:00:00:01.04512/2</td>
<td>2</td>
</tr>
<tr>
<td>1005129</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>P</td>
<td>26b</td>
<td>TREE1</td>
<td>36112214.00:00:00:00:00:01.00052/2</td>
<td>2</td>
</tr>
<tr>
<td>1005129</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Systems
show ipx traffic

Command Mode
User.

Description
Displays the number and type of IPX packets transmitted and received.

Syntax
show ipx traffic

Sample Output
The following is an example of the output that displays after you enter the show ipx traffic command.

Rcvd:  3260 total, 56 format errors, 0 checksum errors, 0 bad hop count, 0 unknown socket, 3204 local destination, 0 NetBIOS
Sent:  14104 generated, 0 forwarded, 57 no route, 1 output errors
Echo:  Rcvd 0 requests, 1 replies
       Sent 1 requests, 0 replies

Systems
Overview

This chapter describes the following commands:

- `ip multicast route-cache aging`
- `ip multicast route-cache hash-mode`
- `ip multicast route-cache max-size`
- `ip multicast route-cache readd-timeout`
- `ip multicast route-cache update-timeout`
- `ip unicast route-cache aging`
- `ip unicast route-cache hash-mode`
- `ip unicast route-cache max-size`
- `ip unicast route-cache update-timeout`
- `ipx route-cache aging`
- `ipx route-cache hash-mode`
- `ipx route-cache max-size`
- `ipx route-cache update-timeout`
- `show ip multicast cache`
- `show ip unicast cache`
- `show ipx cache`
ip multicast route-cache aging

**Command Mode**  
Global Configuration.

**Description**  
Enables aging of IP multicast forwarding cache entries. The `no` form of this command disables aging. The default state is enabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip multicast route-cache aging</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip multicast route-cache aging</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example enables aging of IP routes in the IP forwarding cache.

```
(configure) # ip multicast route-cache aging
```

**Systems**  
**ip multicast route-cache hash-mode**

**Command Mode**  
Global Configuration.

**Description**  
Configures the ip multicast route cache hashing mode. The no form of this command restores the default, which is sa-da.

**Syntax**

| To Configure: | ip multicast route-cache hash-mode {da-only | sa-da} |
|---------------|--------------------------------------------------|
| To Restore Default: | [no] ip multicast route-cache hash-mode |

**Table 14-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| {da-only | sa-da}     | Enter the hash table lookup mode for IP multicast. Choices include:  
  • da-only - Destination address only.  
  • sa-da - Source Address-Destination Address. |

**Sample Output**  
The following example enables IP multicast route cache hash mode for the source address/destination address.

```
(configure)# ip multicast route-cache hash-mode sa-da
```

**Systems**  
**ip multicast route-cache max-size**

**Command Mode**
Global Configuration.

**Description**
Sets a maximum limit on the number of entries in the ip multicast route cache per forwarding chip. The no form of this command restores the default, which is 15000 entries.

**Syntax**

<table>
<thead>
<tr>
<th><strong>To Configure:</strong></th>
<th>ip multicast route-cache max-size <code>&lt;multicast-max-size&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Restore Default:</strong></td>
<td>[no] ip multicast route-cache max-size</td>
</tr>
</tbody>
</table>

**Table 14-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;multicast-max-size&gt;</code></td>
<td>The maximum number of entries allowed in the multicast route cache.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables IP multicast route cache max size of 10000 entries.

```
(configure)# ip multicast route-cache max-size 10000
```

**Systems**
ip multicast route-cache readd-timeout

Command Mode
Global Configuration.

Description
This command is useful only for networks that are designed to route multicast traffic. If the switch is not running IGMP-Only or a multicast routing protocol on multiple IP interfaces, this command has no useful effect.

Upon receiving the first frame of a new flow, the forwarding entry cache software is designed to enter a cache entry in the hardware. If the forwarding entry cache software continues to receive frames for the same flow for a certain length of time, the software assumes that the hardware was unable to install the forwarding entry when last programmed, and will therefore make a new attempt.

The length of time for which the software waits before attempting to re-add the forwarding entry is called the readd-timeout. The readd-timeout should be kept small so that a missed attempt at installing a forwarding entry will be recovered from quickly.

The default timeout is 2 seconds, and the range of adjustment is from 2 to 60 seconds. The no command restores the default setting.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip multicast route-cache readd-timeout &lt;timeout-interval&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip multicast route-cache readd-timeout</td>
</tr>
</tbody>
</table>

Table 14-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;timeout-interval&gt;</td>
<td>Time, in seconds, that the software will wait before allowing an attempt to re-add a multicast forwarding entry.</td>
</tr>
</tbody>
</table>
Sample Output

The following example sets the IP multicast route cache re-add timeout interval to 10 seconds.

(configure)# ip multicast route-cache readd-timeout 10

Systems

**ip multicast route-cache update-timeout**

**Command Mode**
Global Configuration.

**Description**
Sets the period of cache invalidation due to aging. The no form of this restores the default of 120 seconds.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip multicast route-cache update-timeout &lt;ip-multicast-period&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip multicast route-cache update-timeout</td>
</tr>
</tbody>
</table>

**Table 14-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-multicast-period&gt;</td>
<td>The period, in seconds, that route cache entries are invalidated. The range is 20 to 360 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the IP multicast route cache aging invalidation period to 200 seconds.

```
(configure)# ip multicast route-cache update-timeout 200
```

**Systems**
ip unicast route-cache aging

Command Mode  Global Configuration.

Description  Enables aging of IP unicast route cache entries. The no form of this command disables aging. The default state is enabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip unicast route-cache aging</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip unicast route-cache aging</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables aging of IP unicast routes in the forwarding cache.

```
(configure)  ip unicast route-cache aging
```

ip unicast route-cache hash-mode

Command Mode  Global Configuration.

Description  Configures the IP unicast route cache hashing mode. The no form of this command restores the default, which is da-only.

Syntax

| To Configure: | ip unicast route-cache hash-mode {da-only | sa-da} |
| To Restore Default: | [no] ip unicast route-cache hash-mode |

Table 14-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{da-only</td>
<td>sa-da}</td>
</tr>
<tr>
<td></td>
<td>• da-only - Destination address only.</td>
</tr>
<tr>
<td></td>
<td>• sa-da - Source Address-Destination Address.</td>
</tr>
</tbody>
</table>

Sample Output  The following example configures the IP unicast route cache for the da-only mode.

(configure)# ip unicast route-cache hash-mode da-only

**ip unicast route-cache max-size**

**Command Mode**  
Global Configuration.

**Description**  
Sets a maximum limit on the number of entries in the ip unicast route cache per forwarding chip. The no form of this command restores the default, which is 15000 entries.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip unicast route-cache max-size &lt;unicast-max-size&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip unicast route-cache max-size</td>
</tr>
</tbody>
</table>

**Table 14-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;unicast-max-size&gt;</td>
<td>Maximum number of entries allowed in the unicast route cache.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example configures IP Unicast forwarding cache max size of 10000.

```
(configure)# ip unicast route-cache max-size 10000
```

**Systems**  
ip unicast route-cache update-timeout

Command Mode  Global Configuration.

Description  Sets the period of ip unicast route cache invalidation due to aging. The no form of this command restores the default of 120 seconds.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip unicast route-cache update-timeout &lt;ip-unicast-period&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip unicast route-cache update-timeout</td>
</tr>
</tbody>
</table>

Table 14-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-unicast-period&gt;</td>
<td>The period, in seconds, that route cache entries are invalidated. The range is 20-360 seconds.</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables the ip unicast route-cache update-timeout command and sets it to 60 seconds.

(configure)# ip unicast route-cache update-timeout 60

ipx route-cache aging

Command Mode  Global Configuration.

Description  Enables and disables IPX route cache aging. The no form of this command disables aging. The default state is enabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ipx route-cache aging</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ipx route-cache aging</td>
</tr>
</tbody>
</table>

Sample Output  The following example disables ipx route cache aging.

(configure) # ipx route-cache aging disabled

ipx route-cache hash-mode

Command Mode
Global Configuration.

Description
Configures the IPX unicast route cache hashing mode. The no form of this command restores the default, which is da-only.

Syntax

| To Configure:                | ipx route-cache hash-mode {da-only | sa-da} |
|------------------------------|---------------------------------------------|
| To Restore Default:         | [no] ipx route-cache hash-mode              |

Table 14-8. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{da-only</td>
<td>sa-da}</td>
</tr>
<tr>
<td></td>
<td>• da-only - destination address only.</td>
</tr>
<tr>
<td></td>
<td>• sa-da - source and destination addresses.</td>
</tr>
</tbody>
</table>

Sample Output
The following example sets ipx route cache hash mode to sa-da.

(configure)# ipx route-cache hash-mode sa-da

Systems
### ipx route-cache max-size

**Command Mode**
Global Configuration.

**Description**
Sets a maximum limit on the number of entries in the IPX route cache. The no form of this command restores the default, which sets IPX route-cache max-size to the default of 15000 entries.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ipx route-cache max-size &lt;ipx-max-size&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ipx route-cache max-size</td>
</tr>
</tbody>
</table>

**Table 14-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipx-max-size&gt;</td>
<td>Maximum number of entries allowed in IPX route cache.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the maximum route cache size to 12000 entries.

```
(configure)# ipx route-cache max-size 12000
```

**Systems**
ipx route-cache update-timeout

Command Mode  Global Configuration.

Description  Sets the period of IPX route cache invalidation due to aging. The no form of this command restores the default of 120 seconds.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ipx route-cache update-timeout &lt;ipx-period&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ipx route-cache update-timeout</td>
</tr>
</tbody>
</table>

Table 14-10. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ipx-period&gt;</td>
<td>The period, in seconds, that route cache entries are invalidated.</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the update timeout period to 3 minutes.

(configure)# ipx route-cache update-timeout 180

### show ip multicast cache

**Command Mode**  
User.

**Description**  
Displays the IP multicast L3 forwarding cache entries.

**Syntax**  
show ip multicast cache

**Sample Output**  
The following examples shows a typical IP multicast cache display:

```
> show ip multicast cache
PRE 6
   Tree is IP_NUL
   Access Rule is None
   Destination Address is 255.0.1.1
   Source Address is 10.0.1.199
   Destination Port is 0
   Source Port is 0
   Comp is DASA
   TTL is 0
   Age is 7
   Filter is Yes
   Destination VLAN is vlan40
   Source VLAN is vlan40
   Mac Address is Derived from DA
   Use is 1
   Priority is 0
   Format is Eth 2System Supported: P550R
```

**Systems**  
show ip unicast cache

Command Mode User

Description Displays the IP unicast L3 forwarding cache entries.

Syntax show ip unicast cache

Sample Output The following example shows a typical IP unicast cache display:

```
> show ip unicast cache
PRE 2
Destination Address is 10.0.4.94
Source Address is 0.0.0.0
Destination Port is 0
Source Port is 0
Comp is DA
TTL is 0
Age is 7
Filter is No
Destination VLAN is vlan40
Source VLAN is n/a
Mac Address is 02:e0:3b:dd:c4:27
Use is 0
Priority is 7
Format is Eth 2
.
.
```

show ipx cache

**Command Mode**    User.

**Description**    Displays the IPX forwarding cache entries.

**Syntax**    show ipx cache

**Sample Output**    The following example shows a typical IPX cache display:

```plaintext
> show ipx cache
PRE 2
Destination Address is 10.0.4.94
Source Address is 0.0.0.0
Destination Port is 0
Source Port is 0
Comp is DA
TTL is 0
Age is 7
Filter is No
Destination VLAN is vlan40
Source VLAN is n/a
Mac Address is 02:e0:3b:dd:c4:27
Use is 0
Priority is 7
Format is Eth 2
```

Overview

This chapter describes the following commands:

- ldap execution-option
- ldap search-base
- ldap server primary
- ldap server secondary
- show ldap
**ldap execution-option**

**Command Mode**  
Global Configuration.

**Description**  
Sets whether Avaya Policy Manager (APM) stops or continues to apply a policy if an error with a command occurs. The default setting is `stop-on-error`.

**Syntax**

<table>
<thead>
<tr>
<th>To Stop:</th>
<th>ldap execution-option stop-on-error</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Continue:</td>
<td>ldap execution-option ignore-errors</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the `ldap execution-option` to `ignore-errors`.

```
(configure)# ldap execution-option ignore-errors
```

**Systems**  
ldap search-base

**Command Mode**
Global Configuration.

**Description**
Defines the Lightweight Directory Access Protocol (LDAP) search base. The `no` form of this command removes a search base definition.

The search base default is `ou=Devices, ou=CajunRules, o=Avaya`.

* **Note:** If LDAP has not been configured, there is no default.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ldap search-base <code>&lt;search-base-dn&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ldap search-base <code>&lt;search-base-dn&gt;</code></td>
</tr>
</tbody>
</table>

**Table 15-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;search-base-dn&gt;</code></td>
<td>The Distinguished Name (DN) that defines the start point of the search.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The name you enter must start and end with quotation marks.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets an LDAP search base to avaya.com.

```
(configure)# ldap search-base "o"
```

**Systems**
**Idap server primary**

**Command Mode**  
Global Configuration.

**Description**  
Changes the primary LDAP server's IP address and port. The **no** form of this command removes the primary LDAP Server's IP Address. The default IP address is: **0.0.0.0**. The default port number is **389**.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ldap server primary <code>&lt;ip-addr&gt;</code> [<code>&lt;port-num&gt;</code>]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ldap server primary</td>
</tr>
</tbody>
</table>

**Table 15-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>The IP address of the primary LDAP server.</td>
</tr>
<tr>
<td><code>&lt;port-num&gt;</code></td>
<td>The port number of the primary LDAP server.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the LDAP server’s primary IP address to 199.93.238.93.

```
(configure)# ldap server primary 199.93.238.93 389
```

**Systems**  
ldap server secondary

Command Mode  Global Configuration.

Description  Changes the secondary LDAP server’s IP Address and port. The no form of this command removes the secondary LDAP Server’s IP Address. The default port number is: 389.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ldap server secondary &lt;ip-addr&gt; [&lt;port-num&gt;]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ldap server secondary</td>
</tr>
</tbody>
</table>

Table 15-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the secondary LDAP server.</td>
</tr>
<tr>
<td>&lt;port-num&gt;</td>
<td>The port number of the secondary LDAP server.</td>
</tr>
</tbody>
</table>

Sample Output  The following example changes the secondary ldap server’s IP address to 199.93.238.94.

(configure)# ldap server secondary 199.93.238.94 389

show ldap

**Command Mode**  User.

**Description**  Displays the current LDAP configuration information.

**Syntax**  show ldap

**Sample Output**  The following example displays the LDAP configuration information.

```
> show ldap
  LDAP Configuration
  -------------------
  Primary LDAP Server IP address: 10.10.9.41
  Primary LDAP Server Port: 389
  Secondary LDAP Server IP address: 10.10.9.42
  Secondary LDAP Server Port: 389
  LDAP Search base: ou=Devices,ou=CajunRules,o=avayactc.com
  Last Change: 22977
  LDAP Producer Signal: 120
  LDAP Consumer Signal: 120
  LDAP Execution Option: ignore-errors
```

16 Logging

Overview

This chapter describes the following commands:

- logging clear
- logging console
- logging history
- logging history size
- logging protocol event
- logging shutdown size
- logging traps
- set syslog
- set syslog facility
- set syslog server_ip
- set syslog severity
- show alarms
- show logging
- show syslog buffer
- show syslog config
logging clear

Command Mode: Global Configuration.

Description: Clears the contents of the event log.

Syntax: logging clear

Sample Output: The following example clears the event log.

```
(configure)# logging clear
Delete Event Log (Y/N) y
Event log has been cleared.
```

logging console

Command Mode  Global Configuration.

Description  Sets the type of syslog messages that are sent to the console. The no form of this command disables the type specified. The default setting is: {system | switch_fabric}

Syntax

| To Enable: | logging console [{start | system | config | temp | resource | fan | power | service_port | user_port | auth_failure | bridge_stat | switch_fabric | ospf | dvmrp | rip | ldap | cli | snmp | appletalk | redundant_cpu | vrrp | unknown_mac | login_status | acl_log | ssl_ssh}]
| To Disable: | no logging console [{start | system | config | temp | resource | fan | power | service_port | user_port | auth_failure | bridge_stat | switch_fabric | ospf | dvmrp | rip | ldap | cli | snmp | appletalk | redundant_cpu | vrrp | unknown_mac | login_status | acl_log | ssl_ssh}]

* Note: Use the logging protocol event command to enable protocol event logging for specific protocols.

Table 16-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Logs starts of the system.</td>
</tr>
<tr>
<td>system</td>
<td>Logs system events.</td>
</tr>
<tr>
<td>config</td>
<td>Logs each configuration change (for example, enabling and disabling ports).</td>
</tr>
<tr>
<td>temp</td>
<td>Logs changes in temperature status. Temperature status messages could precede a switch shutdown, and are often critical.</td>
</tr>
<tr>
<td>resource</td>
<td>Logs changes in system resources.</td>
</tr>
<tr>
<td>fan</td>
<td>Logs fan status changes. Fan failures will eventually lead to overheating the system. The fan status message provides a good early warning for a failure that could eventually cause the switch to shut down.</td>
</tr>
<tr>
<td>power</td>
<td>Logs the addition or removal of a power supply</td>
</tr>
</tbody>
</table>
service_port  Logs status changes in service ports.
   Use the set port category command to set a port as a service port. For information on this command, see Chapter 21. This feature makes it possible for you to use different notification levels for critical (service ports), if desired.

user_port  Logs status changes in user ports.
   Use the set port category command to set a port as a user port. For information on this command, see Chapter 21. This feature makes it possible for you to use different notification levels for critical (service ports), if desired.

auth_failure  Logs authentication failures. This is a security-related feature used to detect unauthorized SNMP activity.

bridge_stat  Logs changes in bridge status.

switch_fabric  Logs failures in the switch fabric. These failures are critical and should be monitored closely.

ospf  Logs OSPF events if OSPF protocol event logging is enabled.

dvmrp  Logs DVMRP events, if DVMRP event logging is enabled.

rip  Logs RIP events if RIP protocol event logging is enabled.

ldap  Logs LDAP events if LDAP protocol event logging is enabled.

cli  Logs CLI events, if CLI event logging is enabled.

snmp  Logs SNMP events, if SNMP protocol event logging is enabled.

appletalk  Logs AppleTalk events if AppleTalk protocol event logging is enabled.

redundant_cpu  Logs changes in status of a redundant CPU. Notification is sent if:
   - The status changes from standby to active or vice versa.
   - The active supervisor loses or establishes contact with the standby supervisor.

vrrp  Logs VRRP events, if VRRP protocol event logging is enabled.

Table 16-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_port</td>
<td>Logs status changes in service ports. Use the set port category command to set a port as a service port. For information on this command, see Chapter 21. This feature makes it possible for you to use different notification levels for critical (service ports), if desired.</td>
</tr>
<tr>
<td>user_port</td>
<td>Logs status changes in user ports. Use the set port category command to set a port as a user port. For information on this command, see Chapter 21. This feature makes it possible for you to use different notification levels for critical (service ports), if desired.</td>
</tr>
<tr>
<td>auth_failure</td>
<td>Logs authentication failures. This is a security-related feature used to detect unauthorized SNMP activity.</td>
</tr>
<tr>
<td>bridge_stat</td>
<td>Logs changes in bridge status.</td>
</tr>
<tr>
<td>switch_fabric</td>
<td>Logs failures in the switch fabric. These failures are critical and should be monitored closely.</td>
</tr>
<tr>
<td>ospf</td>
<td>Logs OSPF events if OSPF protocol event logging is enabled.</td>
</tr>
<tr>
<td>dvmrp</td>
<td>Logs DVMRP events, if DVMRP event logging is enabled.</td>
</tr>
<tr>
<td>rip</td>
<td>Logs RIP events if RIP protocol event logging is enabled.</td>
</tr>
<tr>
<td>ldap</td>
<td>Logs LDAP events if LDAP protocol event logging is enabled.</td>
</tr>
<tr>
<td>cli</td>
<td>Logs CLI events, if CLI event logging is enabled.</td>
</tr>
<tr>
<td>snmp</td>
<td>Logs SNMP events, if SNMP protocol event logging is enabled.</td>
</tr>
<tr>
<td>appletalk</td>
<td>Logs AppleTalk events if AppleTalk protocol event logging is enabled.</td>
</tr>
<tr>
<td>redundant_cpu</td>
<td>Logs changes in status of a redundant CPU. Notification is sent if:</td>
</tr>
<tr>
<td></td>
<td>- The status changes from standby to active or vice versa.</td>
</tr>
<tr>
<td></td>
<td>- The active supervisor loses or establishes contact with the standby supervisor.</td>
</tr>
<tr>
<td>vrrp</td>
<td>Logs VRRP events, if VRRP protocol event logging is enabled.</td>
</tr>
</tbody>
</table>
Logging Systems


Table 16-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>unknown_mac</td>
<td>Logs unknown MAC addresses if received.</td>
</tr>
<tr>
<td>login_status</td>
<td>Logs User login or logout.</td>
</tr>
<tr>
<td>acl_log</td>
<td>Logs packets that match access control rules.</td>
</tr>
<tr>
<td>ssl_ssh</td>
<td>Logs SSH events.</td>
</tr>
</tbody>
</table>

3 of 3
logging history

Command Mode  
Global Configuration.

Description  
Sets the type of syslog messages that are sent to the event log and shutdown log. The no form of this command disables the type specified. The default setting is {start | system | config | temp | resource | fan | power | service_port | user_port | auth_failure | bridge_stat | switch_fabric | snmp | redundant_cpu | unknown_mac | login_status | acl_log}.

Syntax

To Enable:  
logging history [{start | system | config | temp | resource | fan | power | service_port | user_port | auth_failure | bridge_stat | switch_fabric | ospf | dvmrp | rip | ldap | cli | snmp | appletalk | redundant_cpu | vrrp | unknown_mac | login_status | acl_log| ssl_ssh}]

To Disable:  
no logging history [logging console [{start | system | config | temp | resource | fan | power | service_port | user_port | auth_failure | bridge_stat | switch_fabric | ospf | dvmrp | rip | ldap | cli | snmp | appletalk | redundant_cpu | vrrp | unknown_mac | login_status | acl_log| ssl_ssh}]

* Note:  Use the logging protocol event command to enable protocol event logging for specific protocols.

Table 16-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Logs starts of the system.</td>
</tr>
<tr>
<td>system</td>
<td>Logs system events.</td>
</tr>
<tr>
<td>config</td>
<td>Logs each configuration change (for example, enabling and disabling ports).</td>
</tr>
<tr>
<td>temp</td>
<td>Logs changes in temperature status. Temperature status messages could</td>
</tr>
<tr>
<td></td>
<td>precede a switch shutdown, and are often critical.</td>
</tr>
<tr>
<td>resource</td>
<td>Logs changes in system resources.</td>
</tr>
<tr>
<td>fan</td>
<td>Logs fan status changes. Fan failures will eventually lead to</td>
</tr>
<tr>
<td></td>
<td>overheating the system. The fan status message provides a good early</td>
</tr>
<tr>
<td></td>
<td>warning for a failure that could eventually cause the switch to shut down.</td>
</tr>
</tbody>
</table>
Logging

**Table 16-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>power</td>
<td>Logs the addition or removal of a power supply</td>
</tr>
<tr>
<td>service_port</td>
<td>Logs status changes in service ports. Use the <code>set port category</code> command to set a port as a service port. For information on this command, see Chapter 21. This feature makes it possible for you to use different notification levels for critical (service ports), if desired.</td>
</tr>
<tr>
<td>user_port</td>
<td>Logs status changes in user ports. Use the <code>set port category</code> command to set a port as a user port. For information on this command, see Chapter 21. This feature makes it possible for you to use different notification levels for critical (service ports), if desired.</td>
</tr>
<tr>
<td>auth_failure</td>
<td>Logs authentication failures. This is a security-related feature used to detect unauthorized SNMP activity.</td>
</tr>
<tr>
<td>bridge_stat</td>
<td>Logs changes in bridge status.</td>
</tr>
<tr>
<td>switch_fabric</td>
<td>Logs failures in the switch fabric. These failures are critical and should be monitored closely.</td>
</tr>
<tr>
<td>ospf</td>
<td>Logs OSPF events if OSPF protocol event logging is enabled.</td>
</tr>
<tr>
<td>dvmrp</td>
<td>Logs DVMRP events, if DVMRP event logging is enabled.</td>
</tr>
<tr>
<td>rip</td>
<td>Logs RIP events if RIP protocol event logging is enabled.</td>
</tr>
<tr>
<td>ldap</td>
<td>Logs LDAP events if LDAP protocol event logging is enabled.</td>
</tr>
<tr>
<td>cli</td>
<td>Logs CLI events, if CLI event logging is enabled.</td>
</tr>
<tr>
<td>snmp</td>
<td>Logs SNMP events, if SNMP protocol event logging is enabled.</td>
</tr>
<tr>
<td>appletalk</td>
<td>Logs AppleTalk events if AppleTalk protocol event logging is enabled.</td>
</tr>
<tr>
<td>redundant_cpu</td>
<td>Logs changes in status of a redundant CPU. Notification is sent if:</td>
</tr>
<tr>
<td></td>
<td>- The status changes from standby to active or vice versa.</td>
</tr>
<tr>
<td></td>
<td>- The active supervisor loses or establishes contact with the standby supervisor.</td>
</tr>
</tbody>
</table>
Table 16-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp</td>
<td>Logs VRRP events, if VRRP protocol event logging is enabled.</td>
</tr>
<tr>
<td>unknown_mac</td>
<td>Logs unknown MAC addresses if received.</td>
</tr>
<tr>
<td>login_status</td>
<td>Logs User login or logout.</td>
</tr>
<tr>
<td>acl_log</td>
<td>Logs packets that match access control rules.</td>
</tr>
<tr>
<td>ssl_ssh</td>
<td>Logs SSH events.</td>
</tr>
</tbody>
</table>

Systems

**logging history size**

**Command Mode**  
Global Configuration.

**Description**  
Change the number of syslog messages stored in the event log. The **no** form of this command resets the number of messages to the default value, which is 512.

**Syntax**

| To Configure:         | logging history size {128 | 512 | 1024 | 2048} |
|----------------------|-----------------------------------|
| To Restore Default:  | no logging history size           |

**Table 16-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{128</td>
<td>512</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example specifies that 1024 messages can be stored in the event log.

```
(configure)# logging history size 1024
```

**Systems**  
**logging protocol event**

**Command Mode**  
Global Configuration.

**Description**  
Sets the categories of the protocol events that generate notifications. If you enable event notification for CLI, SNMP, RIP, OSPF, DVMRP, LDAP, Apple Talk, or VRRP, you must set which categories of the protocol events generate notifications.

*Important:* If enabled, protocol event logging displays system messages that help Avaya Technical Support troubleshoot network problems. Avaya recommends that logging of protocol events be enabled only during troubleshooting sessions. If protocol event logging is enabled during normal network operation, the switch may display messages that users may incorrectly interpret as indications of protocol failures.

*Note:* Enabling logging of protocol events may cause the event log to rapidly fill with protocol events.

The no command disables event notification for the specified category of protocol events. The default setting is that all protocol events are disabled.

**Syntax**

| To Enable: | logging protocol event {rip | ospf | dvmrp | ldap | cli | snmp | appletalk | vrrp} {fault | error | warning | info | trace | debug} |
|------------|--------------------------------------------------|
| To Disable: | no logging protocol event {rip | ospf | dvmrp | ldap | cli | snmp | appletalk | vrrp} {fault | error | warning | info | trace | debug} |
Table 16-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{rip</td>
<td>ospf</td>
</tr>
<tr>
<td>{fault</td>
<td>error</td>
</tr>
<tr>
<td></td>
<td>fault—Serious errors that can cause a system crash, for example, panic.</td>
</tr>
<tr>
<td></td>
<td>error—Serious errors that will not cause a system crash but can contribute to protocol problems.</td>
</tr>
<tr>
<td></td>
<td>warning—Noncritical errors.</td>
</tr>
<tr>
<td></td>
<td>info—Event details.</td>
</tr>
<tr>
<td></td>
<td>trace—Packet traces. If you enable trace logging, all protocol packets sent and received are logged as protocol events.</td>
</tr>
<tr>
<td></td>
<td>debug—Event messages used to troubleshoot a network problem.</td>
</tr>
</tbody>
</table>

Sample Output

The following example logs all of the LDAP fault messages.

```
(configure)# logging protocol event ldap fault
Completed set configuration for protocol events.
```

Systems

logging shutdown size

Command Mode
Global Configuration.

Description
Change the number of syslog messages stored in the shutdown log. The no form of this command resets the number of messages to the default value, which is 16.

Syntax

| To Configure:     | logging shutdown size {16 | 32 | 64} |
|-------------------|---------------------------------------|
| To Restore Default: | no logging shutdown size              |

Table 16-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{16</td>
<td>32</td>
</tr>
</tbody>
</table>

Sample Output
The following example sets the number of syslog messages to be stored in the shutdown log to 64.

```
(configure) # logging shutdown size 64
```

Systems
logging traps

Command Mode
Global Configuration.

Description
Sets the type of syslog messages that are sent to SNMP trap receivers. The **no** form of this command disables the type specified. The default setting is: `{start | system | config | temp | resource | fan | power | service_port | auth_failure | bridge_stat | switch_fabric | redundant_cpu | unknown_mac | snmp}`.

Syntax

| To Enable: | `logging traps {start | system | config | temp | resource | fan | power | service_port | user_port | auth_failure | bridge_stat | switch_fabric | redundant_cpu | unknown_mac | snmp | login_status}` |
|-------------|-------------------------------------------------|
| To Disable: | `no logging traps {start | system | config | temp | resource | fan | power | service_port | user_port | auth_failure | bridge_stat | switch_fabric | redundant_cpu | unknown_mac | snmp | login_status}` |

Table 16-6. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Logs starts of the system.</td>
</tr>
<tr>
<td>system</td>
<td>Logs system events.</td>
</tr>
<tr>
<td>config</td>
<td>Logs each configuration change (for example, enabling and disabling ports).</td>
</tr>
<tr>
<td>temp</td>
<td>Logs changes in temperature status. Temperature status messages could precede a switch shutdown, and are often critical.</td>
</tr>
<tr>
<td>resource</td>
<td>Logs changes in system resources.</td>
</tr>
<tr>
<td>fan</td>
<td>Logs fan status changes. Fan failures will eventually lead to overheating the system. The fan status message provides a good early warning for a failure that could eventually cause the switch to shut down.</td>
</tr>
<tr>
<td>power</td>
<td>Logs the addition or removal of a power supply</td>
</tr>
</tbody>
</table>
The following example sends all of the switch_fabric syslog messages to the SNMP trap receivers.

configure) # logging traps switch_fabric

Systems

set syslog

Command Mode  Global Configuration.

Description  Enables or disables syslog event reporting. The default setting is disabled.

Syntax  set syslog {enable | disable}

Systems  P580 and P882.
**set syslog facility**

**Command Mode**  
Global Configuration.

**Description**  
Sets the event types, also called “facilities,” for which syslog events are generated.

The `no` command stops generating syslog events for the event type that you specify. The default setting is `{system | config | switch_fabric}`.

**Syntax**

| To Enable: | set syslog facility { start | system | config | temp | resource | fan | service_port | user_port | power | bridge_stat | switch_fabric | ospf | rip | ldap | appletalk | auth_failure | redundant_cpu | dvmrp | cli | snmp | unknown_mac | vrrp | login_status | acl_log | ssl_ssh | all } |
|------------|--------------------------------------------------|
| To Disable: | no set syslog facility { start | system | config | temp | resource | fan | service_port | user_port | power | bridge_stat | switch_fabric | ospf | rip | ldap | appletalk | auth_failure | redundant_cpu | dvmrp | cli | snmp | unknown_mac | vrrp | login_status | acl_log | ssl_ssh | all } |

*Note:* Use the `logging protocol event` command to enable protocol event logging for specific protocols.

**Table 16-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>start</td>
<td>Logs starts of the system.</td>
</tr>
<tr>
<td>system</td>
<td>Logs system events.</td>
</tr>
<tr>
<td>config</td>
<td>Logs each configuration change (for example, enabling and disabling ports).</td>
</tr>
<tr>
<td>temp</td>
<td>Logs changes in temperature status. Temperature status messages could precede a switch shutdown, and are often critical.</td>
</tr>
<tr>
<td>resource</td>
<td>Logs changes in system resources.</td>
</tr>
</tbody>
</table>
Logging

**Table 16-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>fan</td>
<td>Logs fan status changes. Fan failures will eventually lead to overheating the system. The fan status message provides a good early warning for a failure that could eventually cause the switch to shut down.</td>
</tr>
<tr>
<td>service_port</td>
<td>Logs status changes in service ports. Use the set port category command to set a port as a service port. For information on this command, see Chapter 21. This feature makes it possible for you to use different notification levels for critical (service ports), if desired.</td>
</tr>
<tr>
<td>user_port</td>
<td>Logs status changes in user ports. Use the set port category command to set a port as a user port. For information on this command, see Chapter 21. This feature makes it possible for you to use different notification levels for critical (service ports), if desired.</td>
</tr>
<tr>
<td>power</td>
<td>Logs the addition or removal of a power supply.</td>
</tr>
<tr>
<td>bridge_stat</td>
<td>Logs changes in bridge status.</td>
</tr>
<tr>
<td>switch_fabric</td>
<td>Logs failures in the switch fabric. These failures are critical and should be monitored closely.</td>
</tr>
<tr>
<td>ospf</td>
<td>Logs OSPF events if OSPF protocol event logging is enabled.</td>
</tr>
<tr>
<td>rip</td>
<td>Logs RIP events if RIP protocol event logging is enabled.</td>
</tr>
<tr>
<td>ldap</td>
<td>Logs LDAP events if LDAP protocol event logging is enabled.</td>
</tr>
<tr>
<td>appltalk</td>
<td>Logs AppleTalk events if AppleTalk protocol event logging is enabled.</td>
</tr>
<tr>
<td>auth_failure</td>
<td>Logs authentication failures. This is a security-related feature used to detect unauthorized SNMP activity.</td>
</tr>
<tr>
<td>redundant_cpu</td>
<td>Logs changes in status of a redundant CPU. Notification is sent if:</td>
</tr>
<tr>
<td></td>
<td>• The status changes from standby to active or vice versa.</td>
</tr>
<tr>
<td></td>
<td>• The active supervisor loses or establishes contact with the standby supervisor.</td>
</tr>
<tr>
<td>dvmrp</td>
<td>Logs DVMRP events, if DVMRP event logging is enabled.</td>
</tr>
</tbody>
</table>
### Table 16-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cli</td>
<td>Logs CLI events, if CLI event logging is enabled.</td>
</tr>
<tr>
<td>snmp</td>
<td>Logs SNMP events, if SNMP protocol event logging is enabled.</td>
</tr>
<tr>
<td>unknown_mac</td>
<td>Logs unknown MAC addresses if received.</td>
</tr>
<tr>
<td>vrrp</td>
<td>Logs VRRP events, if VRRP protocol event logging is enabled.</td>
</tr>
<tr>
<td>login_status</td>
<td>Logs User login or logout.</td>
</tr>
<tr>
<td>acl_log</td>
<td>Logs packets that match access control rules.</td>
</tr>
<tr>
<td>ssl_ssh</td>
<td>Logs SSH events.</td>
</tr>
<tr>
<td>all</td>
<td>Logs all event types.</td>
</tr>
</tbody>
</table>

**Systems**

P580 and P882.
set syslog server_ip

**Command Mode**
Global Configuration.

**Description**
Sets the IP addresses of remote syslog servers to which you want syslog events forwarded.

The `no` command stops forwarding syslog events to the syslog server that you specify.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set syslog server_ip &lt;ip_address&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no set syslog server_ip &lt;ip_address&gt;</td>
</tr>
</tbody>
</table>

**Table 16-8. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip address&gt;</td>
<td>The IP address of the remote syslog server to which you want syslog events forwarded. You can specify a maximum of three remote syslog servers.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
set syslog severity

**Command Mode**
Global Configuration.

**Description**
Sets the severity of error messages that you want logged. Table 16-9 describes the different syslog severity levels. The switch logs error messages of the severity that you set and of all higher severities. For example, if you set the severity to **Warning**, error messages of severities Warning, Error, Alert, and Emergency are logged.

The default setting is error.

**Table 16-9. Syslog Severity Levels**

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>System Unusable</td>
</tr>
<tr>
<td>Alert</td>
<td>Immediate action needed</td>
</tr>
<tr>
<td>Error</td>
<td>Error Condition</td>
</tr>
<tr>
<td>Warning</td>
<td>Warning Condition</td>
</tr>
<tr>
<td>Normal</td>
<td>Normal but significant condition</td>
</tr>
<tr>
<td>Informational</td>
<td>Informational message only</td>
</tr>
</tbody>
</table>

**Syntax**

```
set syslog severity {emergency | alert | error | warning | normal | informational}
```

* **Note:** See Table 16-9 for an explanation of each keyword.

**Systems**
P580 and P882.
show alarms

Command Mode
User.

Description
Displays the contents of the active alarm table.

Syntax
show alarms

Sample Output
The following example displays the contents of the active alarm table.

> show alarms
---------- Active Alarms ----------
-------------------------------------------------------
ID : 2 : Controller Failure : Missing (3) : Redundant Controller
-------------------------------------------------------
ID : 10 : Port Status : No Link (5) : Port 3.1
-------------------------------------------------------
ID : 11 : Port Status : No Link (5) : Port 3.2
-------------------------------------------------------
ID : 12 : Port Status : No Link (5) : Port 4.1
-------------------------------------------------------

Systems
Chapter 16

show logging

Command Mode  User.

Description  Displays the contents of the event or shutdown log. The number of events can be specified at the end of the command.

Syntax  show logging [shutdown] [<num-events>]

Table 16-10. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>shutdown</td>
<td>Displays the contents of the shutdown log.</td>
</tr>
<tr>
<td>&lt;num-events&gt;</td>
<td>The number of log messages to display.</td>
</tr>
</tbody>
</table>

Sample Output  The following example displays 25 messages from the shutdown log.

> show logging shutdown 25

<table>
<thead>
<tr>
<th>Log ID</th>
<th>Event ID</th>
<th>TimeStamp</th>
<th>Severity</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>61</td>
<td>3</td>
<td>03-Sep-05 12:00:16</td>
<td>Informative(20)</td>
<td>0</td>
</tr>
<tr>
<td>======</td>
<td>Set minimum password length to 0 succeeded</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>3</td>
<td>03-Sep-05 12:00:16</td>
<td>Informative(20)</td>
<td>0</td>
</tr>
<tr>
<td>======</td>
<td>Set account timeout limit to 60 succeeded</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>3</td>
<td>03-Sep-05 12:00:16</td>
<td>Informative(20)</td>
<td>0</td>
</tr>
<tr>
<td>======</td>
<td>Set login attempts succeeded</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>1</td>
<td>03-Sep-05 12:00:16</td>
<td>Informative(20)</td>
<td>0</td>
</tr>
<tr>
<td>======</td>
<td>System cold started at 03-Sep-05 12:00:15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>18</td>
<td>03-Sep-05 12:00:16</td>
<td>Informative(20)</td>
<td>0</td>
</tr>
<tr>
<td>======</td>
<td>The CPU in slot 1 is the Active CPU for this switch</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>9</td>
<td>03-Sep-05 12:00:16</td>
<td>Warning(40)</td>
<td>0</td>
</tr>
<tr>
<td>55</td>
<td>9</td>
<td>03-Sep-05 12:00:16</td>
<td>Warning(40)</td>
<td>0</td>
</tr>
</tbody>
</table>

--More--

show syslog buffer

Command Mode User.

Description Displays events in the syslog buffer.

Syntax show syslog buffer

Sample Output

<table>
<thead>
<tr>
<th>log ID</th>
<th>Event ID</th>
<th>TimeStamp</th>
<th>Facility</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>03-Sep-22 02:55</td>
<td>Configuration</td>
<td>Informative(20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>RIP global config updated</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>03-Sep-22 02:55</td>
<td>Configuration</td>
<td>Informative(20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DVMRP global config updated</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>03-Sep-22 02:55</td>
<td>Configuration</td>
<td>Informative(20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IGMP global config updated</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>5</td>
<td>03-Sep-22 02:55</td>
<td>Status</td>
<td>Informative(20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Arp refresh set to Disable</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>03-Sep-22 09:55</td>
<td>Power Status</td>
<td>Warning(40)</td>
</tr>
<tr>
<td>6</td>
<td>18</td>
<td>03-Sep-22 09:55</td>
<td>Redundant CPUS</td>
<td>Informative(20)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The CPU in slot 1 is the Active CPU for this switch.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>03-Sep-22 09:55</td>
<td>Fan Status</td>
<td>Alarm(60)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fan Unit Operational: Fan 1. [Module Fan Pair 1]</td>
<td></td>
</tr>
</tbody>
</table>

--More--

Systems P580 and P882.
show syslog config

**Command Mode**  
User.

**Description**  
Displays the current configuration for syslog event reporting.

**Syntax**  
show syslog config

**Sample Output**  
Syslog Server: Enabled  
Severity: informational  
Server IP:  
135.35.93.125  
Facility:  
start  
system  
config  
temp  
resource  
fan  
service_port  
user_port  
power  
bridge_stat  
switch_fabric  
ospf  
rip  
ldap  
appletalk  
auth_failure  
redundant_cpu  
dvmrp  
cli  
snmp  
unknown_mac  
vrrp  
login_status  
ac1_log  
ssl_ssh

**Systems**  
P580 and P882.
17 Module

Overview

This chapter describes the following commands:

- reset-module
- set module name
- set module notes
- show module
reset-module

Command Mode  Global Configuration.

Description  Resets an individual module other than the supervisor module.

Syntax  reset-module <mod-num>

Table 17-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The module number that you want to reset.</td>
</tr>
</tbody>
</table>

* Note: You cannot reset an individual module from the Web Agent.

Sample Output  The following example resets the module in slot 4.

(configure) # reset-module 4

set module name

Command Mode  Global Configuration.

Description  Creates the name for a module. Omitting the <mod-name> variable clears the module name.

Syntax  set module name <mod-num> [<mod-name>]

Table 17-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module whose name is to be cleared or set.</td>
</tr>
<tr>
<td>&lt;mod-name&gt;</td>
<td>Specifies the name of the module. If the module name is not specified, any previous name for the module is cleared.</td>
</tr>
</tbody>
</table>

Sample Output  The following example creates the name of the module in slot 3.

(configure)# set module name 3 "MIS dept module"
Module 3 name set

set module notes

**Command Mode**
Global Configuration.

**Description**
Creates a notes page for a module. Omitting the `<mod-notes>` variable clears the module notes.

**Syntax**
```
set module notes <mod-num> [<mod-notes>]
```

**Table 17-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module whose notes are to be cleared or set.</td>
</tr>
<tr>
<td><code>&lt;mod-notes&gt;</code></td>
<td>Specifies the notes to be assigned to the module. If the module notes are not specified, any previous notes for the module are cleared.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the note page for the module in slot 3.

```
(configure) # set module notes 3 "This module was installed on 01/21/02"
Module 3 notes set
```

**Systems**
show module

Command Mode
User.

Description
Displays information about the modules installed in the switch chassis. The default state displays information for all modules installed in the switch.

Syntax
show module [<mod-num>]

Table 17-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module whose information is to be displayed.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays information about the modules installed in the switch chassis.

```
> show module
Module Model Number Base Type Ports Fabric Ports
------- ---------------------------- ------------------
1 M5500R-SUP Supervisor 0 1/1, 1/FORE
Name Notes
---------------------------------------------------------
Module 1
Module Model Number Base Type Ports Fabric Ports
------- ---------------------------- ------------------
3 M5502-1000SX-FGigabit 2 3/1, 3/2
Name Notes
---------------------------------------------------------
Module 3
Module Model Number Base Type Ports Fabric Ports
------- ---------------------------- ------------------
4 M5502-1000LX-FGigabit 2 4/1, 4/2
Name Notes
---------------------------------------------------------
```

Systems
show module inventory

Command Mode
User.

Description
Displays information about the hardware in the switch chassis.

Syntax
show module inventory {<mod-num> | bp | all}

Table 17-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of the module.</td>
</tr>
<tr>
<td>bp</td>
<td>The backplane.</td>
</tr>
<tr>
<td>all</td>
<td>All hardware in the chassis.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays the inventory information for the module in slot 5.

> show module-inventory 5
Inventory version: 3
Serial Number: 040C0004
Module Base Type: 0000
Module Type: 001F
MAC Address: 02:e0:3B:04:dc:8c
Model Number: 8024-100TX
Hardware Version:
Date of Manufacture:
Name of Manufacturer: Jabil
Power Consumption: 0050

Systems
Overview

This chapter describes the following commands:

- `set huntgroup internal-error-shutdown`
- `set internal-error-threshold`
- `set port internal-error-shutdown`
- `set port network-error-detection`
- `show huntgroup internal-error-config`
- `show port internal-error-config`
- `show port network-error detection`
set huntgroup internal-error-shutdown

**Command Mode**   
Global Configuration.

**Description**   
Globally enables or disables internal error detection and recovery (IEDR) for all ports in hunt groups.

* Note: All ports that have IEDR enabled, whether they are administratively disabled or enabled, assume the hunt group IEDR setting if they are placed in a hunt group. If a port has IEDR enabled before you place it in a hunt group, the `show port internal-error-config` command displays the port as IEDR-enabled regardless of the huntgroup IEDR setting. However, the port in fact assumes the hunt group IEDR setting (whatever that setting is).

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set huntgroup internal-error-shutdown enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set huntgroup internal-error-shutdown disable</td>
</tr>
</tbody>
</table>

**Sample Output**   
The following example globally enables IEDR on all ports on a huntgroup.

```bash
(configure) # set huntgroup internal-error-shutdown enable
```

**Systems**   
set internal-error-threshold

**Command Mode**
Global Configuration.

**Description**
Sets the IEDR threshold for internal errors. When a port reaches this threshold, it is shut down.

By default this threshold is set to 10 internal errors in a 5-second time period. You can set the threshold to any number between 5 and 500 internal errors in a 5-second time period. This setting is global for all ports that have been enabled for IEDR including ports configured for Hunt groups.

**Syntax**
set internal-error-threshold <internal-threshold>

**Table 18-1. Parameters, Keywords, Argument**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;internal-threshold&gt;</td>
<td>The threshold at which a port is shutdown if it has IEDR enabled. This threshold is measured in a number of errors per 5-second time period. The valid range is 5 to 500 internal errors. The default setting is 10.</td>
</tr>
</tbody>
</table>

**Systems**
set port internal-error-shutdown

Command Mode  Global Configuration.

Description  Enables or disables internal error detection and recovery (IEDR) on a port or ports

Syntax

| To Enable: | set port internal-error-shutdown { <mod-num> | <mod-swport-spec> | all-ports } enable |
| To Disable: | set port internal-error-shutdown { { <mod-num> | <mod-swport-spec> } | all-ports } disable |

Table 18-2. Parameters, Keywords, Argument

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| { <mod-num> | <mod-swport-spec> } | The slot number of the module, and, either port number, or range of port numbers. Enter the port ranges in the format Px-Py. For example:  
  - To specify port 1 on the module in slot 3, enter 3/1.  
  - To specify ports 1 through 5 on the module in slot 3, enter 3/1-5. |
| all-ports | Enables or disables IEDR on all ports on all modules in the switch. |

Sample Output  The following example enables IEDR on all ports on the module in slot 3.

(configure) # set port internal-error-shutdown 3 enable

set port network-error-detection

Command Mode
Global Configuration.

Description
Configure network error detection and recovery (NEDR) for a port or ports.

Syntax

| To Enable: | set port network-error-detection <mod-port-range> [action {notify | disable-port}] [rising-threshold <rising-threshold-value>] [falling-threshold <falling-threshold-value>] [interval <interval seconds>] |
| To Disable: | network-error-detection { <mod-port-range> | all} action off |

Table 18-3. Parameters, Keywords, Argument

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| <mod-port-range> | The slot number of the module, and, either port number, or range of port numbers. Enter the port ranges in the format Px-Py. For example:  
- To specify port 1 on the module in slot 3, enter 3/1.  
- To specify ports 1 through 5 on the module in slot 3, enter 3/1-5. |
| all | Disables NEDR on all ports on all modules in the switch.  
**all** can be used only with **off**. |
| action {notify | disable-port | off} | Action that NEDR performs when the rate of errors exceeds the threshold. The options are:  
**notify** - Logs the event in the event log  
**disable-port** - Disables the port and logs the event in the event log.  
**Note:** A port will be disabled if the rate of errors equals or exceeds the threshold. Make sure a redundant protocol is configured.  
**off** - Disables NEDR on the port or ports that you specify.  
The default setting is **notify**. |
The following command sets NEDR on ports 1-5 on module 3.

(configure)# set port network-error-detection 3/1-5

**Systems**


**Table 18-3. Parameters, Keywords, Argument**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| <rising-threshold value> | The rising threshold. The number of CRC errors that triggers NEDR to log an event in the event log or disable the port. The default setting is 100 (minimum is 1; maximum is 65535).  
**Note:** If you set the rising threshold value and the falling threshold value close together, events may be logged more often if the Notify option is selected. |
| <falling-threshold value> | The falling threshold. After exceeding the rising threshold, NEDR does not log another event in the event log until the rate of CRC errors falls below the falling threshold and then exceeds the rising threshold again. The default setting is half the rising threshold value (minimum is 0; maximum is 65535).  
**Note:** If you set the rising threshold value and the falling threshold value close together, events may be logged more often if the Notify option is selected. |
| <interval-seconds>       | How often NEDR checks the number of errors occurring against the thresholds. Enter a number of seconds. The default setting is 2 seconds (minimum is 1; maximum is 65535). |
### show huntgroup internal-error-config

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Displays the IEDR setting (enabled or disabled) for hunt groups and the global IEDR threshold setting.</td>
</tr>
<tr>
<td>Syntax</td>
<td>show huntgroup internal-error-config</td>
</tr>
</tbody>
</table>
show port internal-error-config

**Command Mode**  
User.

**Description**  
Displays a list of the ports that have IEDR enabled, the IEDR setting for hunt groups, and the global IEDR threshold setting.

**Syntax**  
show port internal-error-config

**Systems**  
show port network-error detection

Command Mode  User.

Description  Displays the ports that have NEDR enabled.

Syntax  show port network-error-detection

19 OSPF

Overview

This chapter describes the following commands:

- area
- area ase-filter
- area default-cost
- area nssa
- area range
- area stub
- area translate-nssa-to-external
- area virtual-link
- ip ospf as-boundary-router
- ip ospf authentication-key
- ip ospf auto-vlink-create
- ip ospf cost
- ip ospf dead-interval
- ip ospf ext-route-metric
- ip ospf hello-interval
- ip ospf max-paths
- ip ospf message-digest-key md5
- ip ospf packet tracing
- ip ospf poll interval
- ip ospf reset-stats
- ip ospf retransmit-interval
- ip ospf router-id
- ip ospf transmit-delay
- network area
- passive-interface
- router ospf
- show ip ospf
- show ip ospf database
- show ip ospf interface
- show ip ospf neighbor
- show ip ospf stats
- show ip ospf virtual-links
- timers lsa-group-pacing
- timers spf
area

Command Mode OSPF Router Configuration.

Description Defines an OSPF Area. To remove an area, use the no form of this command.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>area &lt;area-id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] area &lt;area-id&gt;</td>
</tr>
</tbody>
</table>

Table 19-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>IP address that represents the area-id for the system.</td>
</tr>
</tbody>
</table>

Sample Output The following command removes the OSPF Area from the indicated router.

```
(configure router:ospf)# no area 10.0.0.123
```

area ase-filter

**Command Mode**
OSPF Router Configuration.

**Description**
Enables the filtering of type 3 ASE LSAs into an OSPF Area. To disable the filtering of type 3 ASE LSAs, use the `no` form of this command.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>area &lt;area-id&gt; ase-filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] area &lt;area-id&gt; ase-filter</td>
</tr>
</tbody>
</table>

**Table 19-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>IP address that represents the area-id for the system.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command enables filtering of type 3 ASE LSAs into the indicated OSPF Area.

```
(configure router:ospf)# area 2.0.0.0 ase-filter
```

**Systems**
area default-cost

**Command Mode** OSPF Router Configuration.

**Description** Defines the cost for routes advertised into stub area by an area border router. To restore the default value, use the no form of this command. The valid range is 1 to 65535. The default setting is 1.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure</th>
<th>area &lt;area-id&gt; default-cost &lt;cost&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default</td>
<td>[no] area &lt;area-id&gt; default-cost</td>
</tr>
</tbody>
</table>

**Table 19-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>A decimal value or IP address that identifies an OSPF area.</td>
</tr>
<tr>
<td>&lt;cost&gt;</td>
<td>A cost value of the area. The valid range is 1 to 65535. The default setting is 1.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following command sets an area default cost of 3 on OSPF set on the specified router.

```
(configure router:ospf)# area 2.0.0.0 default-cost 3
```

The following command removes an area default cost from OSPF set on the specified router.

```
(configure router:ospf)# no area 2.0.0.0 default-cost
```

area nssa

Command Mode  OSPF Router Configuration.

Description  Configure an area as a Not So Stubby Area (NSSA). To remove the NSSA distinction from the area, use the no form of this command.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>area &lt;area-id&gt; nssa</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] area &lt;area-id&gt; nssa</td>
</tr>
</tbody>
</table>

Table 19-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>A decimal value or IP address that identifies an OSPF area. Use no area &lt;area-id&gt; to remove an area from the software configuration.</td>
</tr>
</tbody>
</table>

Sample Output

The following command sets nssa on the indicated area.

(configure router:ospf)# area 2.0.0.0 nssa

The following command removes nssa from the indicated area.

(configure router:ospf)# no area 2.0.0.0 nssa

Systems

area range

**Command Mode**
OSPF Router Configuration.

**Description**
Consolidates and summarizes routes at an area boundary. To disable this function, use the no form of this command.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>area &lt;area-id&gt; range &lt;ip-address&gt; &lt;mask&gt; [no-advertisement]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] area &lt;area-id&gt; range &lt;ip-address&gt; &lt;mask&gt;</td>
</tr>
</tbody>
</table>

**Table 19-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>IP address that represents the area-id for the system.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IP address of the area range.</td>
</tr>
<tr>
<td>&lt;mask&gt;</td>
<td>IP address of the mask for the area range.</td>
</tr>
<tr>
<td>[no-advertisement]</td>
<td>Suppresses advertisements of this summary. When suppressing, advertisements of IP routes in this range are also suppressed.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command sets an area range on the indicated area.

```
(configure router:ospf)# area 2.0.0.0 range 10.0.5.123 255.0.0.0
```

**Systems**
area stub

Command Mode
OSPF Router Configuration.

Description
Defines an area as a stub area. Use the no form of this command to remove the stub area distinction.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>area &lt;area-id&gt; stub</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] area &lt;area-id&gt; stub</td>
</tr>
</tbody>
</table>

Table 19-6. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>IP address that represents the area-id for the system.</td>
</tr>
</tbody>
</table>

Sample Output
The following command removes a stub area on the indicated area.

(configure router:ospf)# no area 2.0.0.0 stub

Systems
area translate-nssa-to-external

**Command Mode**   OSPF Router Configuration.

**Description**   Enables the translation of type 7 LSAs into type 5. To disable this feature use the `no` form of this command.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>area <code>&lt;area-id&gt;</code> translate-nssa-to-external</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] area <code>&lt;area-id&gt;</code> translate-nssa-to-external</td>
</tr>
</tbody>
</table>

**Table 19-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;area-id&gt;</code></td>
<td>IP address that represents the area-id for the system.</td>
</tr>
</tbody>
</table>

**Sample Output**   The following command enables the translation of Type 7 LSAs into Type 5 on the indicated OSPF area.

```
(configure router:ospf)# area 2.0.0.0 translate-nssa-to-external
```

area virtual-link

**Command Mode**  
OSPF Router Configuration.

**Description**  
Defines an OSPF virtual link. To remove a virtual link, use the no form of this command.

**Syntax**

**To Configure:**

```
area <area-id> virtual-link <router-id> [hello-interval <hello-interval>] [retransmit-interval <retransmit-interval>] [dead-interval <dead-interval>] [transit-delay <transit-delay>] [{authentication-key <passwd> | message-digest-key <key-id> md5 <key>}]
```

**To Disable:**

```
[no] area <area-id> virtual-link <router-id>
```

**Table 19-8. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;area-id&gt;</td>
<td>IP address that represents the area-id for the system.</td>
</tr>
<tr>
<td>&lt;router-id&gt;</td>
<td>Router ID associated with the virtual link neighbor. The router ID appears in the show ip ospf display. It is internally derived by each router from the router's interface IP addresses. This value must be entered in the format of an IP address. There is no default.</td>
</tr>
<tr>
<td>&lt;hello-interval&gt;</td>
<td>Time in seconds between the hello packets that the Cisco IOS software sends on an interface. Unsigned integer value to be advertised in the software’s hello packets. The value must be the same for all routers and access servers attached to a common network. The default is 10 seconds.</td>
</tr>
<tr>
<td>&lt;retransmit-interval&gt;</td>
<td>Time in seconds between link state advertisement retransmissions for adjacencies belonging to the interface. Expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The default is 5 seconds.</td>
</tr>
<tr>
<td>&lt;dead-interval&gt;</td>
<td>Time in seconds that a software’s hello packets are not seen before its neighbors declare the router down. Unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.</td>
</tr>
</tbody>
</table>
Table 19-8. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;transit-delay&gt;</td>
<td>Estimated number of seconds it takes to transmit a link state update packet over this virtual link. The value range is 1-3600. The default is 1.</td>
</tr>
<tr>
<td>&lt;passwd&gt;</td>
<td>Password to be used by neighboring routers. Any continuous string of characters that you can enter from the keyboard up to 8 bytes long. This string acts as a key that will allow the authentication procedure to generate or verify the authentication field in the OSPF header. This key is inserted directly into the OSPF header when originating routing protocol packets. A separate password can be assigned to each network on a per-interface basis. All neighboring routers on the same network must have the same password to be able to route OSPF traffic.</td>
</tr>
<tr>
<td>message-digest-key</td>
<td>Key identifier and password to be used by neighboring routers and this router for MD5 authentication. The key id is a number in the range 1 to 255. The key is an alphanumeric string of up to 16 characters. All neighboring routers on the same network must have the same key identifier and key to be able to route OSPF traffic. There is no default value.</td>
</tr>
<tr>
<td>md5 &lt;key&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Systems

ip ospf as-boundary-router

Command Mode Global Configuration.

Description * Important: This command is not supported by v6.0 and later application software.

Version 6.0 and later application software automatically detects the ASBR status:

- If route redistribution filters are configured for OSPF, the ASBR status is enabled.
- If all interfaces on the switch are in an OSPF stub area, the ASBR status is disabled, regardless of whether route redistribution filters are configured.


In earlier versions of application software, this command specifies if the router is an autonomous-system boundary router (ASBR). Use the no form of this command to disable ASBR status. The default state is disabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip ospf as-boundary-router</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip ospf as-boundary-router</td>
</tr>
</tbody>
</table>

ip ospf authentication-key

Command Mode

Interface Configuration.

Description

Assign a password to be used by neighboring routers that are using OSPF’s simple password authentication. To remove a previously assigned OSPF password, use the no form of this command.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip ospf authentication-key  &lt;password&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip ospf authentication-key</td>
</tr>
</tbody>
</table>

Table 19-9. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;password&gt;</td>
<td>Any continuous string of characters that can be entered from the keyboard up to 8 bytes in length.</td>
</tr>
</tbody>
</table>

Sample Output

The following command assigns the password “abc” as the authentication key.

(config-if:intf3)# ip ospf authentication-key “abc”

The following command removes the password “abc” as the authentication key.

(config-if:intf3)# no ip ospf authentication-key

Systems

ip ospf auto-vlink-create

Command Mode: Global Configuration.

Description: Enables the automatic creation of virtual links. Use the no form of this command to disable this behavior.

Syntax:

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip ospf auto-vlink-create</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip ospf auto-vlink-create</td>
</tr>
</tbody>
</table>

Sample Output: The following command enables the automatic creation of virtual links.

(config-if:intf3)# ip ospf auto-vlink-create

**ip ospf cost**

**Command Mode** Interface Configuration.

**Description** Specifies the cost of sending a packet on an interface. The no form of this command restores the default setting of 1. The valid range is 1 to 65534.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip ospf cost &lt;cost&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip ospf cost</td>
</tr>
</tbody>
</table>

**Table 19-10. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;cost&gt;</td>
<td>Unsigned integer value expressed as the link state metric. It can be a value in the range 1 to 65534.</td>
</tr>
</tbody>
</table>

**Sample Output** The following command enables the cost of sending a packet on an interface to 100.

```
(config-if:intf3)# ip ospf cost 100
```

### ip ospf dead-interval

**Command Mode**

Interface Configuration.

**Description**

Sets the dead interval time for neighbors to declare this router down. Dead interval is the time that hello packets are not seen. This value must be the same for all routers attached to a common network. The value range is 1-65535 seconds. The default setting is 40 seconds.

To return to the default time, use the `no` form of this command.

**Syntax**

```
To Configure:    ip ospf dead-interval <seconds>
To Restore Default: [no] ip ospf dead-interval
```

**Table 19-11. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td>Time in seconds of how long hello packets must be unseen before the neighbor declares the router down. This value must be the same for all routers attached to a common network. The value range is 1-65535 seconds. The default setting is 40 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following command sets the dead interval time to 60 seconds.

```
(config-if:intf3)# ip ospf dead-interval 60
```

**Systems**

ip ospf ext-route-metric

Command Mode: Global Configuration.

Description: Sets the metric type used for external routes to type1 or type2. Use the no form of this command to restore default values. The default values are:

- local (type1)
- rip (type2)
- static-hp (type2)
- static-lp (type-2)

Syntax:

| To Configure:                         | ip ospf ext-route-metric {local | rip | static-hp | static-lp} {type1 | type2} |
|---------------------------------------|--------------------------------------------------------------------------------|
| To Restore Default:                   | [no] ip ospf ext-route-metric {local | rip | static-hp | static-lp} |

Table 19-12. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Specifies whether imported local routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies whether imported RIP routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics.</td>
</tr>
<tr>
<td>static-hp</td>
<td>Specify whether imported high preference static routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics.</td>
</tr>
<tr>
<td>static-lp</td>
<td>Specify whether imported low preference static routes are advertised in OSPF with type 1 (internal) or type 2 (external) metrics.</td>
</tr>
</tbody>
</table>

Sample Output: The following command sets the metric type for RIP used for external routes to Type 2

```
(configure)# ip ospf ext-route-metric rip type2
```

Chapter 19

**ip ospf hello-interval**

**Command Mode**
Interface Configuration.

**Description**
Specifies the hello interval time. The hello interval time is the time between hello packets that the router sends on the interface. The value range is 1 to 65535. The default setting is 10. The **no** command restores the default setting.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip ospf hello-interval <code>&lt;seconds&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td><code>[no] ip ospf hello-interval</code></td>
</tr>
</tbody>
</table>

**Table 19-13. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td>Unsigned integer that specifies the interval in seconds. The value must be the same for all nodes on a specific network. The value range is 1 to 65535. The default setting is 10.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command sets the Hello interval time to 60 seconds.

```
(config-if:intf3)# ip ospf hello-interval 60
```

**Systems**
**ip ospf max-paths**

**Command Mode**  Global Configuration.

**Description**  Configures the maximum number of Simple Path First (SPF) paths that OSPF can use. The path range values are:

- Minimum **640** (default)
- Maximum **16000**

Use the **no** form of this command to restore the default value (**640**).

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip ospf max-paths <code>&lt;paths&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip ospf max-paths</td>
</tr>
</tbody>
</table>

**Sample Output**  The following command sets the maximum number of SPF paths to 1000.

(configure)# **ip ospf max-paths 1000**

**ip ospf message-digest-key md5**

**Command Mode**
- Interface Configuration.

**Description**
- Enables OSPF MD5 authentication.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip ospf message-digest-key &lt;key-id&gt; md5 &lt;key&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip ospf message-digest-key &lt;keyid&gt; md5 &lt;key&gt;</td>
</tr>
</tbody>
</table>

**Table 19-14. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;key-id&gt;</td>
<td>An identifier in the range 1 to 255.</td>
</tr>
<tr>
<td>&lt;key&gt;</td>
<td>Alphanumeric password of up to 16 bytes.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following command enables OSPF MD5 authentication on interface 3 with a key ID of 155, and a key labeled jerry.

```
(config-if:intf3)# ip ospf message-digest-key 155 md5 jerry
```

**Systems**

ip ospf packet tracing

Command Mode  Global Configuration.

Description  Enables or disables OSPF packet tracing.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip ospf packet tracing</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip ospf packet tracing</td>
</tr>
</tbody>
</table>

Sample Output

The following command enables packet tracing.

(configure)# ip ospf packet tracing

Systems

ip ospf poll interval

Command Mode
Interface Configuration.

Description
Specifies the poll interval time. The valid range is 1 to 3600 seconds. The default setting is 120 seconds. The no command restores the default setting.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip ospf poll-interval &lt;seconds&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip ospf poll-interval</td>
</tr>
</tbody>
</table>

Table 19-15. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;seconds&gt;</td>
<td>Time in seconds between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is 1 to 3600 seconds.</td>
</tr>
</tbody>
</table>

Sample Output
The following command sets the poll interval time on interface 123 to 2000 seconds.

```
(config-if:123)# ip ospf poll-interval 2000
```

Systems
ip ospf reset-stats

Command Mode  Global Configuration.

Description  Resets the OSPF global statistics.

Syntax  ip ospf reset-stats

Sample Output  The following command resets the OSPF global statistics.

  (configure)# ip ospf reset-stats

ip ospf retransmit-interval

Command Mode
Interface Configuration.

Description
Specifies the time between link state advertisement retransmissions for adjacencies belonging to the interface. The no command restores the default setting. The value range is 1-3600. The default is 5.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip ospf retransmit-interval &lt;seconds&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip ospf retransmit-interval</td>
</tr>
</tbody>
</table>

Table 19-16. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;seconds&gt;</td>
<td>Time in seconds between retransmissions. It must be greater than the expected round-trip delay between any two routers on the attached network. The range is 1 to 3600 seconds. The default is 5 seconds.</td>
</tr>
</tbody>
</table>

Sample Output
The following command specifies the time retransmit interval time on interface 123 to 2000 seconds.

(config-if:123)# ip ospf retransmit-interval 2000

Systems
**ip ospf router-id**

**Command Mode**  
Global Configuration.

**Description**  
Sets the router-id for the system. Use the no command to restore the default setting (the lowest IP address configured on the system).

* **Note:** OSPF must be disabled for this command to take effect. If OSPF is enable on the system the change will not take effect until OSPF is stopped and started again.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip ospf router-id &lt;router-id&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip ospf router-id</td>
</tr>
</tbody>
</table>

**Table 19-17. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>router-id</td>
<td>IP address that represents the router-id for the system.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following command sets the router id for interface 123 to 10.0.8.123.

```
(config-if:123)# ip ospf router-id 10.0.7.123
```

**Systems**  
**ip ospf transmit-delay**

**Command Mode**  
Interface Configuration.

**Description**  
Sets the estimated time it takes to transmit a link state update packet on the interface. The range is 1 to 3600 seconds. The default is 1 second. To restore the default value, use the `no` form of this command.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th><code>ip ospf transmit-delay &lt;seconds&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td><code>[no] ip ospf transmit-delay</code></td>
</tr>
</tbody>
</table>

**Sample Output**  
The following command sets the transmit delay time on interface 123 to 1000 seconds.

```
(config-if:123)# ip ospf transmit-delay 1000
```

**Systems**  

---

**Table 19-18. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td>Time in seconds that it takes to transmit a link state update. The range is 1 to 3600 seconds. The default is 1 second.</td>
</tr>
</tbody>
</table>
**network area**

**Command Mode**
OSPF Router Configuration.

**Description**
Defines the interfaces on which OSPF runs and defines an area ID for those interfaces. To disable OSPF routing for interfaces defined with the `<ip-address> < wildcard-mask >` pair, use the `no` form of this command.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>network <code>&lt;ip-address&gt; &lt; wildcard-mask &gt; area &lt;area-id&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] network <code>&lt;ip-address&gt; &lt; wildcard-mask &gt; area &lt;area-id&gt;</code></td>
</tr>
</tbody>
</table>

**Table 19-19. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip address&gt;</code></td>
<td>IP address of the interface on which OSPF runs.</td>
</tr>
<tr>
<td><code>&lt;wildcard-mask&gt;</code></td>
<td>The inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask. This parameter specifies a range of IP addresses. For example, to specify all IP addresses in the 10.10.70 subnet, enter <code>10.10.70.0 0.0.0.255</code>.</td>
</tr>
<tr>
<td><code>&lt;area-id&gt;</code></td>
<td>Area ID for the interface.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command defines network area on the interface running at 10.0.7.123 and with area ID 1.1.1.1.

```plaintext
(configure router:ospf)# network 10.0.7.123 255.0.0.0 area 1.1.1.1
```

**Systems**
**passive-interface**

**Command Mode**
OSPF Router Configuration.

**Description**
Prevents OSPF from sending routing updates across the network. To disable passive interface, use the `no` form of this command.

**Syntax**

| To Enable:              | passive-interface {<interface-name> | <ip-address>} |
|-------------------------|---------------|
| To Disable:             | [no] passive-interface {<interface-name> | <ip-address>} |

**Table 19-20. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-name&gt;</td>
<td>Name of the interface on which OSPF runs.</td>
</tr>
<tr>
<td>&lt;ip-address&gt;</td>
<td>IP address of the interface on which OSPF runs.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command enables passive interface on the interface labeled boston with an ip address of 10.0.7.123.

```
(configure router:ospf)# passive-interface boston 10.0.7.123
```

**Systems**
## router ospf

**Command Mode**
Global Configuration.

**Description**
Enables the OSPF protocol on this system. The `no` form of this command disables it globally. The default is `disabled`.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>router ospf</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] router ospf</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables OSPF routing.

```
(configure)# router ospf
```

**Systems**
show ip ospf

Command Mode
User.

Description
Displays general information about OSPF routing.

Syntax
show ip ospf

Sample Output
The following example displays general information about OSPF routing.

> show ip ospf
Routing Process OSPF with ID 45.0.0.0
Supports only single TOS0 0 route
It is an area border and autonomous system boundary router
Redistributing External Routes from rip with metric TYPE 2
Number of areas in this router is 2
Area 0.0.0.0
Number of Interfaces in this area 2
SPF algorithm executed 53 times
Area 1.0.0.0
Number of Interfaces in this area 1
SPF algorithm executed 47 times

Systems
**show ip ospf database**

**Command Mode**  User.

**Description**  Displays lists of information related to the OSPF database for a specific router.

**Syntax**  

```
show ip ospf database [{asbr-summary | router | network | summary | nssa-external | external}]
```

**Sample Output**  

The following command displays the OSPF database for router ID 10.0.1.45.

```
> show ip ospf database
OSPF Router with ID 10.0.1.45

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Type</th>
<th>LSA ID</th>
<th>Router ID</th>
<th>Sequence</th>
<th>age</th>
<th>Cksm</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>1</td>
<td>10.0.1.45</td>
<td>10.0.1.45</td>
<td>8000000e</td>
<td>296</td>
<td>5375</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>3</td>
<td>10.0.2.0</td>
<td>10.0.1.45</td>
<td>8000000e</td>
<td>335</td>
<td>52b8</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>1</td>
<td>10.0.1.45</td>
<td>10.0.1.45</td>
<td>8000000b</td>
<td>297</td>
<td>6268</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>3</td>
<td>10.0.1.0</td>
<td>10.0.1.45</td>
<td>8000000e</td>
<td>336</td>
<td>5dae</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>3</td>
<td>0.0.0.0</td>
<td>10.0.1.45</td>
<td>80000002</td>
<td>331</td>
<td>2bf8</td>
</tr>
</tbody>
</table>
```


---

**Table 19-21. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>asbr-summary</td>
<td>Displays information only about the autonomous system boundary router summary LSAs. Optional.</td>
</tr>
<tr>
<td>external</td>
<td>Displays information only about the external LSAs. Optional.</td>
</tr>
<tr>
<td>network</td>
<td>Displays information only about the network LSAs. Optional.</td>
</tr>
<tr>
<td>nssa-external</td>
<td>Displays information only about the NSSA external LSAs. Optional.</td>
</tr>
<tr>
<td>router</td>
<td>Displays information only about the router LSAs. Optional.</td>
</tr>
</tbody>
</table>

show ip ospf interface

**Command Mode**  
User.

**Description**  
Displays the OSPF-related interface information.

**Syntax**  
show ip ospf interface [<interface-name>]

**Table 19-22. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-name&gt;</td>
<td>The OSPF interface name.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following command displays the OSPF-related information for interface intf5.

```
> show ip ospf interface intf5
Ethernet intf5 is up, line protocol is up
Internet Address 10.0.5.45, Mask 255.255.255.0,
Area 0.0.0.0
AS Router ID 45.0.0.0
Network Type BROADCAST, COST 1
State BACKUP-DR, Priority 1
DRId 43.0.0.0, IpAddress 10.0.5.43
BDR ipAddress 10.0.5.45
Timer Intervals Configured:
Hello 10
Dead 40
wait 40
Retransmit 5
Transit 1
Neighbor count 1, Adjacent Neighbor count 1
Adjacent with neighbor 43.0.0.0 neighbor’s ipaddr
  10.0.5.43
```

**Systems**  
**show ip ospf neighbor**

**Command Mode**  
User.

**Description**  
Displays OSPF-neighbor information on a per-interface basis.

**Syntax**  
```
show ip ospf neighbor [{<interface-name> | <neighbor-id>}][detail]
```

**Sample Output**  
The following command displays OSPF neighbor information for the interface labeled 123.

```
> show ip ospf neighbor
Nbr-Id Priority State  Router ID  Type
----------------- ----- -------------- 
43.0.0.0 1        FULL  10.0.5.43  BROADCAST
43.0.0.0 1        FULL  10.0.3.43  BROADCAST
43.0.0.0 1        FULL  10.0.6.43  BROADCAST
```

**Table 19-23. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface-name&gt;</td>
<td>The OSPF interface name.</td>
</tr>
<tr>
<td>&lt;neighbor-id&gt;</td>
<td>Neighbor ID.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays all neighbors given in detail (list all neighbors).</td>
</tr>
</tbody>
</table>

**Systems**  
show ip ospf stats

Command Mode User.

Description Displays OSPF statistics.

Syntax show ip ospf stats

Sample Output The following command displays OSPF statistics.

> show ip ospf stats
Osfp Global Stats
Osfp state: Active
num of new lsa received 165801
num of new lsa transmitted 76872
num of external lsa count 30
lsachecksum 950158

<table>
<thead>
<tr>
<th>Area Id</th>
<th>Spf Runs</th>
<th>ABR Count</th>
<th>LSA Count</th>
<th>ASBR Count</th>
<th>LSA CSum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>424</td>
<td>6</td>
<td>113</td>
<td>6</td>
<td>003BAC12</td>
</tr>
<tr>
<td>172.172.172.0</td>
<td>424</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0000DBD2</td>
</tr>
<tr>
<td>192.168.89.0</td>
<td>423</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>00008F3B</td>
</tr>
<tr>
<td>192.168.140.0</td>
<td>423</td>
<td>3</td>
<td>120</td>
<td>3</td>
<td>0039E693</td>
</tr>
<tr>
<td>192.168.190.0</td>
<td>395</td>
<td>0</td>
<td>71</td>
<td>0</td>
<td>0022FCB7</td>
</tr>
</tbody>
</table>

show ip ospf virtual-links

Command Mode
User.

Description
Displays parameters that explain the current state of OSPF virtual links.

Syntax
show ip ospf virtual-links

Sample Output
The following command displays parameters about the current state of the virtual links to the switch.

   (configure)# show ip ospf virtual-link
   Virtual link to router 43.0.0.0 is up
   Transit area 1.0.0.0 via interface, Cost of using 1
   Transit Delay is 1 seconds
   Timer Intervals Configured:
   Hello 10
   Dead 40
   wait 40
   Retransmit 5
   Transit 1

Systems
timers lsa-group-pacing

Command Mode
Global Configuration.

Description
Sets the number of LSAs that should be processed at one time, during a SPF calculation. The valid range is 1000 to 16000. The default setting is 1000. Use the no form of this command to restore the default value.

This command helps you gauge how much CPU time is devoted to the SPF calculation at one time.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>timers lsa-group-pacing &lt;lsa-group-size&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] timers lsa-group-pacing</td>
</tr>
</tbody>
</table>

Table 19-24. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;lsa-group-size&gt;</td>
<td>The link state advertisement group size. The range is 1000 to 16000. The default setting is 1000.</td>
</tr>
</tbody>
</table>

Sample Output
The following command sets the LSA timers to 1500.

(configure)# timers lsa-group-pacing 1500

Systems
timers spf

Command Mode Global Configuration.

Description Configures the delay time (seconds) between runs of OSPF’s SPF calculation. Use the no form of this command to restore the default (3 seconds). The valid range is 3 to 65535.

Syntax

```
To Configure:    timers spf <spf-holdtime>
To Restore Default:    [no] timers spf
```

Table 19-25. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;spf-holdtime&gt;</td>
<td>The time in seconds of the delay between runs of OSPF’s SPF calculation. The range is:</td>
</tr>
<tr>
<td></td>
<td>minimum - 3</td>
</tr>
<tr>
<td></td>
<td>maximum - 65535</td>
</tr>
</tbody>
</table>

Sample Output The following command sets the spf holdtime to 60 seconds.

```
(configure)# timers spf 60
```

20 Policy

Overview

This chapter describes the following commands:

- access-list
- ip access-group
- ip access-list
- ip acl-logging
- ip acl-logging logging-interval
- show access-group
- show access-lists
- show acl-match-timer
- show ip access-lists
access-list

Command Mode
Global Configuration.

Description
Creates a rule in an access control list (ACL). The rule that you set is applied on all of the ports on the switch.

* Note: You must enable the ACL on which you want to set a rule. Only one ACL can be enabled at a time.

The no command deletes an ACL rule or ACL.

Syntax

| To Create a Standard ACL Rule: | access-list <access-list-name> <access-list-index> [permit [{use-priority <priority> | use-diffserv [mask] | remark-diffserv <dscp> [mask] | use-l2}] | deny | fwd1 | fwd2 | fwd3 | fwd4 | fwd5 | fwd6 | fwd7 | fwd8} {<source-ip-addr> <source-wildcard> | any | host <source-ip-addr>} |
| To Create an Extended ACL Rule: | access-list <access-list-name> <access-list-index> [permit [{use-priority <priority> | use-diffserv [mask] | remark-diffserv <dscp> [mask] | use-l2}] | deny | fwd1 | fwd2 | fwd3 | fwd4 | fwd5 | fwd6 | fwd7 | fwd8} <protocol-id> {<source-ip-addr> <source-wildcard> | any | host <source-ip-addr>} [{lt <port> | eq <port> | gt <port> | range <port> <port>}] {<dest-ip-addr> <dest-wildcard> | any | host <dest-ip-addr>} [{lt <port> | eq <port> | gt <port> | range <port> <port>} [established] |
| To Remove an ACL Rule or ACL: | no access-list <access-list-name> [<access-list-index>] |
## Table 20-1. Parameters, Keywords, and Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;access-list-name&gt;</code></td>
<td>A unique name that identifies the access control list.</td>
</tr>
<tr>
<td><code>&lt;access-list-index&gt;</code></td>
<td>The rule number within the access list. Index numbers can be 1 through 512.</td>
</tr>
<tr>
<td>permit</td>
<td>Forwards the packet without changing its priority.</td>
</tr>
<tr>
<td>use-priority</td>
<td>Assigns the default layer 3 priority that you define in the following <code>&lt;priority&gt;</code> parameter to the packet.</td>
</tr>
<tr>
<td><code>&lt;priority&gt;</code></td>
<td>The default layer 3 priority. Enter a number between 0 and 7.</td>
</tr>
<tr>
<td>use-diffserv</td>
<td>Classifies traffic by the DSCP in the packet.</td>
</tr>
<tr>
<td>[mask]</td>
<td>Masks the three least significant bits of the DSCP. If you mask the three least significant bits of the DSCP, the switch recognizes the remaining bits as the precedence field of the type of service (TOS) field and classifies the packets accordingly.</td>
</tr>
<tr>
<td>remark-diffserv</td>
<td>Replaces the DSCP in the packet with the DSCP that you enter for the following <code>&lt;dscp&gt;</code> parameter. The switch uses the DSCP that you enter for the <code>&lt;dscp&gt;</code> parameter to classify the packet.</td>
</tr>
<tr>
<td><code>&lt;dscp&gt;</code></td>
<td>The specific DSCP to replace the existing DSCP. The range is 0-63.</td>
</tr>
<tr>
<td>use-l2</td>
<td>Classifies traffic by the layer 2 priority of the packet. If you enter <strong>use-l2</strong>, the switch ignores the layer 3 default priorities and DiffServ priorities.</td>
</tr>
<tr>
<td>deny</td>
<td>Blocks the packet.</td>
</tr>
</tbody>
</table>
Table 20-1. Parameters, Keywords, and Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>fwd1</td>
<td>The priority that you want to set. The number following the fwd specifies the priority. The fwdx arguments are 1-based, while the queue priorities are 0-based. Consequently, the 1-based priorities are converted to 0-based priorities by the Queue Classification and Queue Servicing features. For example, to specify a priority of 0, enter fwd1. These keywords serve the same function as the use-priority &lt;priority&gt; keyword and argument.</td>
</tr>
<tr>
<td>&lt;protocol-id&gt;</td>
<td>The ID of the protocol that you want to assign a priority to. RFC 1700 defines the protocol IDs.</td>
</tr>
<tr>
<td>&lt;source-ip-addr&gt;</td>
<td>The source IP address of the subnet or host to which you want to assign a priority.</td>
</tr>
<tr>
<td>&lt;source-wildcard&gt;</td>
<td>The inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask. This parameter specifies a range of IP address. For example, to specify all IP addresses in the 10.10.70 subnet, enter 10.10.70.0 0.0.0.255.</td>
</tr>
<tr>
<td>any</td>
<td>A source of 0.0.0.0 and a source-wildcard of 255.255.255.255</td>
</tr>
<tr>
<td>host &lt;source-ip-addr&gt;</td>
<td>The source IP address that you want to assign a priority to.</td>
</tr>
<tr>
<td>[{lt &lt;port&gt;</td>
<td>eq &lt;port&gt;</td>
</tr>
<tr>
<td>&lt;dest-ip-addr&gt;</td>
<td>The destination IP address of the subnet or host that you want to assign a priority to.</td>
</tr>
</tbody>
</table>
Table 20-1. Parameters, Keywords, and Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;dest-wildcard&gt;</td>
<td>The inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask. This parameter specifies a range of IP address. For example, to specify all IP addresses in the 10.10.70 subnet, enter <code>10.10.70.0 0.0.0.255</code>.</td>
</tr>
<tr>
<td>any</td>
<td>A destination of 0.0.0.0 and a destination-wildcard of 255.255.255.255</td>
</tr>
<tr>
<td>host &lt;dest-ip-addr&gt;</td>
<td>The destination IP address that you want to assign a priority to.</td>
</tr>
<tr>
<td>![port]</td>
<td>A destination port or range of destination ports that pass data between two hosts or switches using the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP). Enter a number between 0 and 65,535. For a complete list of well-known port numbers (specifically in relation to the destination port), see the following URL: <a href="http://www.iana.org/assignments/port-numbers">http://www.iana.org/assignments/port-numbers</a></td>
</tr>
<tr>
<td>[established]</td>
<td>Permits TCP connections to be established that match the rule.</td>
</tr>
</tbody>
</table>

Sample Output: Standard ACL Rules

The following table provides examples of standard ACL rules.

Table 20-2. Sample Standard ACL Rules

<table>
<thead>
<tr>
<th>To. . .</th>
<th>Enter. . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use the DSCP in the packet to classify all traffic that has a source IP address in the 10.10.60 subnet.</td>
<td>access-list MyAccessList1 4 permit use-diffserv mask 10.10.60.0 0.0.0.255</td>
</tr>
<tr>
<td>• Mask the three least significant bits of the DSCP.</td>
<td></td>
</tr>
<tr>
<td>Assign a priority of 7 to all traffic that has a source IP address in the 10.10.70 subnet.</td>
<td>access-list MyAccessList1 5 permit use-priority 7 10.10.70.0 0.0.0.255</td>
</tr>
</tbody>
</table>
Table 20-2. Sample Standard ACL Rules

<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Replace the existing DSCP with a DSCP of 5 for all traffic that has a source IP address in the 10.10.80 subnet.</td>
<td>access-list MyAccessList1 6 permit remark-diffserv 5 mask 10.10.80.0 0.0.0.255</td>
</tr>
<tr>
<td>• Mask the three least significant bits of the DSCP</td>
<td></td>
</tr>
<tr>
<td>Use the layer 2 priority of the packet to classify all traffic that has a source address in the 11.11.11 subnet</td>
<td>access-list MyAccessList1 7 permit use-l2 11.11.11.0 0.0.0.255</td>
</tr>
<tr>
<td>Use the DSCP in the packet to classify all traffic that has a source IP address of 199.93.239.168</td>
<td>access-list MyAccessList1 8 permit use-diffserv host 199.93.239.168</td>
</tr>
<tr>
<td>• Use the DSCP in the packet to classify all traffic that has a source IP address of 3.3.3.3</td>
<td>access-list MyAccessList1 9 permit use-diffserv mask host 3.3.3.3</td>
</tr>
<tr>
<td>• Mask the three least significant bits of the DSCP</td>
<td></td>
</tr>
<tr>
<td>Assign a priority of 2 to all traffic that has a source IP address of 1.1.1.1</td>
<td>access-list MyAccessList1 10 permit use-priority 2 host 1.1.1.1</td>
</tr>
<tr>
<td>Block all traffic that has a source IP address is 10.1.0.55</td>
<td>access-list MyAccessList1 11 deny 10.1.0.55</td>
</tr>
</tbody>
</table>

Table 20-3. Sample Extended ACL Rules

<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the DSCP in the packet to classify all traffic that has a:</td>
<td>access-list MyAccessList2 1 permit use-diffserv ip host 199.93.239.168 1.1.1.0 0.0.0.255</td>
</tr>
<tr>
<td>• Source IP address of 199.93.239.168</td>
<td></td>
</tr>
<tr>
<td>• Destination address in the 1.1.1 subnet</td>
<td></td>
</tr>
</tbody>
</table>
Table 20-3. Sample Extended ACL Rules

<table>
<thead>
<tr>
<th>To . . . Continued</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the DSCP in the packet to classify all traffic that has a:</td>
<td>access-list MyAccessList2 2 permit use-diffserv mask ip 3.0.0.0 0.255.255.255 5.0.0.0 0.255.255.255</td>
</tr>
<tr>
<td>• Source IP address in the 3.0 subnet</td>
<td></td>
</tr>
<tr>
<td>• Destination address in the 5.0 subnet</td>
<td></td>
</tr>
<tr>
<td>• Mask the three least significant bits of the DSCP</td>
<td></td>
</tr>
<tr>
<td>Assign a priority of 2 to all TCP traffic that has a:</td>
<td>access-list MyAccessList2 3 permit use-priority 2 tcp 1.1.0.0 0.0.255.255 gt 24 6.6.0.0 0.0.255.255 eq 23</td>
</tr>
<tr>
<td>• Source IP address in the 1.1 subnet</td>
<td></td>
</tr>
<tr>
<td>• Source port that is greater than 24</td>
<td></td>
</tr>
<tr>
<td>• Destination IP address in the 6.6 subnet</td>
<td></td>
</tr>
<tr>
<td>• Destination port of 23</td>
<td></td>
</tr>
<tr>
<td>• Replace the existing DSCP of packets with a DSCP of 12 for all traffic that has a source IP address of 199.93.238.83.</td>
<td>access-list MyAccessList2 4 permit remark 12 mask ip host 199.93.238.83 any</td>
</tr>
<tr>
<td>• Mask the three least significant bits of the DSCP.</td>
<td></td>
</tr>
<tr>
<td>Replace the existing DSCP of the packet with a DSCP of 24 for all ICMP traffic that has a:</td>
<td>access-list MyAccessList2 5 permit remark-diffserv 24 icmp host 2.2.2.2 host 4.4.4.4</td>
</tr>
<tr>
<td>• Source IP address of 2.2.2.2</td>
<td></td>
</tr>
<tr>
<td>• Destination IP address of 4.4.4.4</td>
<td></td>
</tr>
<tr>
<td>Assign a priority of 6 to all TCP traffic that has a:</td>
<td>access-list MyAccessList2 6 permit use-priority 6 tcp 10.10.10.0 0.0.0.255 11.11.11.0 0.0.0.255 eq 1</td>
</tr>
<tr>
<td>• Source IP address in the 10.10.10 subnet</td>
<td></td>
</tr>
<tr>
<td>• Destination IP address in the 11.11.11 subnet</td>
<td></td>
</tr>
<tr>
<td>• Destination port of 1</td>
<td></td>
</tr>
<tr>
<td>Use the layer 2 priority in the packet to classify all UDP traffic</td>
<td>access-list MyAccessList2 7 permit use-l2 udp any any</td>
</tr>
</tbody>
</table>
Table 20-3. Sample Extended ACL Rules

<table>
<thead>
<tr>
<th>To . . . Continued</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use the layer 2 priority in the packet to classify all TCP traffic that has a:</td>
<td>access-list MyAccessList2 8 permit use-l2 tcp 5.5.5.0 0.0.0.255 6.6.6.0 0.0.0.255 lt 2 established</td>
</tr>
<tr>
<td>— Source IP address in the 5.5.5 subnet</td>
<td></td>
</tr>
<tr>
<td>— Destination IP address in the 6.6.6 subnet</td>
<td></td>
</tr>
<tr>
<td>— Destination port that is less than 2</td>
<td></td>
</tr>
<tr>
<td>• Permit TCP connections that meet this criteria</td>
<td></td>
</tr>
<tr>
<td>• Use the DSCP to classify all UDP traffic that has a:</td>
<td>access-list MyAccessList2 9 permit use-diffserv mask udp host 7.7.7.7 host 8.8.8.8 range 33 44</td>
</tr>
<tr>
<td>— Source IP address of 7.7.7.7</td>
<td></td>
</tr>
<tr>
<td>— Destination IP address of 8.8.8.8</td>
<td></td>
</tr>
<tr>
<td>— Destination port between 33 and 44</td>
<td></td>
</tr>
<tr>
<td>• Mask the three least significant bits of the DSCP</td>
<td></td>
</tr>
<tr>
<td>• Assign a priority of 7 to all TCP traffic that has a:</td>
<td>access-list MyAccessList2 10 permit use-priority 7 tcp host 9.9.9.9 host 3.3.3.3 range 55 66 established</td>
</tr>
<tr>
<td>— Source IP address of 9.9.9.9</td>
<td></td>
</tr>
<tr>
<td>— Destination IP address of 3.3.3.3</td>
<td></td>
</tr>
<tr>
<td>— Destination port between 55 and 66</td>
<td></td>
</tr>
<tr>
<td>• Permit TCP connections that meet this criteria</td>
<td></td>
</tr>
</tbody>
</table>

Systems

ip access-group

Command Mode
Global Configuration

Description
Enables an access control list (ACL) and optionally sets the default action to deny.

The `default-action-deny` option is a global setting and is not available in the Web Agent. If you use the CLI to enable the `default-action-deny` option and then use the Web Agent to enable a different ACL, the `default-action-deny` option remains enabled. When this option is enabled, the switch blocks all traffic that does not match an access rule in the enabled ACL.

⚠️ CAUTION:

Do not use the Web Agent to enable a different ACL if the default-action-deny option is enabled. Because the option remains enabled, you can unexpectedly lose connectivity to the switch.

To ensure that you never inadvertently lose all connectivity to the switch, you can add an access rule that always permits a specific connection. You must add the rule to all ACLs on the switch, though, so that regardless of the ACL that is enabled, the `default-action-deny` option does not block the connection.

For example, to ensure that you can always connect to the switch from a PC that has an IP address of 192.168.10.10, add the following access rule to all ACLs on the switch: `ip access-list <access-list-name> <access-list-index> permit 192.168.10.10 0.0.0.0`.

The `no` form of this command disables the access control list. The default action is by default set to `permit`.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip access-group <code>&lt;access-list-name&gt;</code> [default-action-deny]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip access-group <code>&lt;access-list-name&gt;</code></td>
</tr>
</tbody>
</table>
**Table 20-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>The name of the access list.</td>
</tr>
</tbody>
</table>
| [default-action-deny]  | Sets the default action to **deny**. When this option is enabled, the switch blocks all traffic that does not match an access rule in the enabled ACL. This option is a global setting and is not available in the Web Agent. If you use the CLI to enable this option and then use the Web Agent to enable a different ACL, the **default-action-deny** option remains enabled. To disable this option, enter **ip access-group** `<group name>` and omit the [default-action-deny] option. For `<group name>`, you can enter:  
  • The name of the currently enabled access list to retain its enabled status.  
  OR  
  • The name of a different access list to enable it. |

**Sample Output**

The following command enables the access-list **fwdrules**:

```
(configure)# ip access-group fwdrules
```

**Systems**

ip access-list

Command Mode Global Configuration.

Description Creates a rule in an access control list (ACL). The rule that you set is applied on all of the ports on the switch.

* Note: You must enable the ACL on which you want to set a rule. Only one ACL can be enabled at a time.

The no command deletes an ACL rule or ACL.

Syntax

<table>
<thead>
<tr>
<th>To Create a Standard ACL Rule:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list &lt;access-list-name&gt; &lt;access-list-index&gt; {permit [{use-priority &lt;priority&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To Create an Extended ACL Rule:</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list &lt;access-list-name&gt; &lt;access-list-index&gt; {permit [{use-priority &lt;priority&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To Remove an ACL Rule or ACL:</th>
</tr>
</thead>
<tbody>
<tr>
<td>no ip access-list &lt;access-list-name&gt; [&lt;access-list-index&gt;]</td>
</tr>
</tbody>
</table>

This command performs the same operation as the access-list command. See that command for explanations of the keywords and variables and for examples.

ip acl-logging

Command Mode: Global Configuration

Description: Enables or disables ACL logging. The default setting for ACL logging is disabled.

Syntax:

To Enable: `ip acl-logging enable <access-list-name> <rule-number>`

To Disable: `ip acl-logging disable <access-list-name> <rule-number>`

Table 20-5. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;access-list-name&gt;</code></td>
<td>The access list that contains the access rule for which you want to enable ACL logging.</td>
</tr>
<tr>
<td><code>&lt;rule-number&gt;</code></td>
<td>The number of the access rule for which you want to enable ACL logging.</td>
</tr>
</tbody>
</table>

ip acl-logging logging-interval

Command Mode  Global Configuration

Description  Sets the interval for ACL logging. The valid range is 1 to 60 seconds. The default setting is 2 seconds.

Syntax  ip acl-logging logging-interval <time-in-seconds>

Table 20-6.  Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Keyword, Argument, or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;time-in-seconds&gt;</td>
<td>The interval at which you want ACL matches logged. Enter an interval from 1 to 60 seconds. The default setting is 2 seconds.</td>
</tr>
</tbody>
</table>

Systems  P580 and P882.
**show access-group**

**Command Mode**  
User.

**Description**  
Displays the enabled access control list.

**Syntax**  
show access-group

**Systems**  
show access-lists

Command Mode
User.

Description
Displays the contents of access lists configured on the switch. The switch displays all access lists by default.

Syntax
show access-lists [<access-list-name>]

Table 20-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>The name of a specific access list to be displayed.</td>
</tr>
</tbody>
</table>

Sample Output
The following command displays the access lists.

> show access-lists
access-list 1 1 deny 0.0.0.0 255.255.255.255
access-list 100 12 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255

Systems
## show acl-match-timer

**Command Mode**  
Global Configuration.

**Description**  
Displays the interval for logging of ACL matches.

**Syntax**  
`show acl-match-timer`

**Sample Output**  
Interval between logging of Access Rule Matches is 2 second(s)

**Systems**  
P580 and P882.
show ip access-lists

Command Mode  
User.

Description  
Displays the contents of the IP access lists configured on the switch. The switch displays all access lists by default.

Syntax  
show ip access-lists [<access-list-name>]

Table 20-8. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>The name of a specific IP access list to be displayed.</td>
</tr>
</tbody>
</table>

Sample Output  
The following command displays the contents of the IP access lists.

> show ip access-lists
  access-list 1 1 deny 0.0.0.0 255.255.255.255
  access-list 100 12 deny ip 0.0.0.0 255.255.255.255
  0.0.0.0 255.255.255.255

Systems  
21 Port

Overview

This chapter describes the following commands:

- clear port counters
- set port 3com-mapping-table
- set port allow-learning
- set port auto-flush
- set port auto-negotiation
- set port auto-negotiation-duplex-advertisement
- set port auto-negotiation-flow-control-advertisement
- set port auto-negotiation-speed-advertisement
- set port auto-vlan-create
- set port category
- set port disable
- set port duplex
- set port edge admin state
- set port enable
- set port flow-control
- set port frame-tags
- set port mirror
- set port internal-error-shutdown
- set port intrusion-trap
- set port intrusion-trap-timer
- set port known-mode
- set port mirror
• set port mirror Fabric_mode2
• set port name
• set port network-error-detection
• set port pace-priority-mode
• set port point-to-point admin status
• set port rate-limit-burst-size
• set port rate-limit-mode
• set port rate-limit-rate
• set port-redundancy
• set port-redundancy name
• set port remote-fault-detect
• set port spanning-tree-mode
• set port speed
• set port trunking-format
• set port vlan
• set port vlan-binding-method
• set port vtp-snooping
• show port
• show port counters
• show port mirror
• show port mirror Fabric_mode2
• show port physical
• show port status
• show port redundancy
clear port counters

Command Mode  Global Configuration.

Description  Clears port ethernet statistics counters. Omitting input clears all port counters on the switch. Selecting a mod-num clears all port counters on the module. By default, the counters of all ports in the switch chassis are cleared.

Syntax  clear port counters [{<mod-num> | <mod-swport-spec>}]

Sample Output  The following command clears the counters for all the ports on the module in slot 3:

    (configure)# clear port counters 3
  Module 3 ports counters cleared

  The following command clears the counters of port 7 on the module in slot 5:

    (configure)# clear port counters 5/7
  Port 5/7 counters cleared


<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module whose port counters are to be cleared.</td>
</tr>
<tr>
<td>&lt;mod-swport-spec&gt;</td>
<td>Specifies a particular port whose counters are to be cleared.</td>
</tr>
</tbody>
</table>
set port 3com-mapping-table

**Command Mode**: Global Configuration.

**Description**: Sets the 3Com mapping table for a specified switch port or all switch ports on a specified module.

**Syntax**: set port 3com-mapping-table {<mod-num> | <mod-swport-range>} [...{<mod-num> | <mod-swport-range>}] <table-name>

**Sample Output**: The following example sets the 3Com Mapping Table assignment for all switch ports on the module in slot 3.

```
(configure)# set port 3com-mapping-table 3 3ComDefault
Port 3Com-mapping-table set: 3/1,3/2
```


### Table 21-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module where the 3Com Mapping Table assignment of each switch is to be set.</td>
</tr>
<tr>
<td><code>&lt;mod-swport-range&gt;</code></td>
<td>Specifies a range of switch ports whose 3Com Mapping Table assignment is to be set.</td>
</tr>
<tr>
<td><code>&lt;table-name&gt;</code></td>
<td>Specifies the name of the 3Com mapping table.</td>
</tr>
</tbody>
</table>
set port allow-learning

Command Mode
Global Configuration.

Description
Disables or enables learning for a specified switch port or all switch ports on a specified module.

Syntax

| To Enable:                                        | set port allow-learning { <mod-num> | <mod-swport-range> }[,...{ <mod-num> | <mod-swport-range> }] enable |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| To Disable:                                      | set port allow-learning { <mod-num> | <mod-swport-range> }[,...{ <mod-num> | <mod-swport-range> }] disable |

Table 21-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the ability of every switch port on that module to learn new VLANs is enabled or disabled.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a range of switch ports whose ability to learn new VLANs is enabled or disabled.</td>
</tr>
</tbody>
</table>

Sample Output
The following example enables VLAN learning for the second switch port on the module in slot 3 and switch ports 7 through 11 on the module in slot 5.

```
(configure)# set port allow-learning 3/2,5/7-11 enable
Port allow-learning set: 3/2,5/7,5/8,5/9,5/10,5/11
```

Systems
set port auto-flush

Command Mode  
Global Configuration.

Description  
When auto-flush is enabled and the link to a port fails, all entries in the address forwarding table that were learned for this port will be marked invalid. The default value for auto-flush is disabled.

Syntax  

| To Enable: | set port auto-flush { <mod-num> | <mod-swport-range> } [...{ <mod-num> | <mod-swport-range> }] enable |
| To Disable: | set port auto-flush { <mod-num> | <mod-swport-range> } [...{ <mod-num> | <mod-swport-range> }] disable |

Table 21-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;module-number&gt;</td>
<td>The module number on which you want to set auto-flush. Auto-flush can be set at the module level or port level.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The port, or port range on which you want to enable auto-flush.</td>
</tr>
</tbody>
</table>

Sample Output  
The following example enables auto-flush for port 2, on module 4.

(configure)# set port auto-flush 4/2 enable
Port auto-flush set successful: 4/2.

Systems  
set port auto-negotiation

Command Mode  Global Configuration.

Description  Enables or disables auto-negotiation on the specified port or ports.

Syntax

| To Enable:      | set port auto-negotiation {<mod-num> | <mod-port-range>}[,...,{<mod-num> | <mod-port-range>}] enable |
|-----------------|----------------------------------------------------------------------------------|
| To Disable:     | set port auto-negotiation {<mod-num> | <mod-port-range>}[,...,{<mod-num> | <mod-port-range>}] disable |

Table 21-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies a module number where auto negotiation for every fast ethernet port on that module is enabled or disabled.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies a range of fast ethernet ports whose ability for auto negotiation is enabled or disabled.</td>
</tr>
</tbody>
</table>

Sample Output

The following example enables auto-negotiation for the second fast ethernet port and ports 7 through 11 on the module in slot 5.

(configure)# set port auto-negotiation 5/2,5-11 enable

Systems

set port auto-negotiation-duplex-advertisement

**Command Mode**  
Global Configuration.

**Description**  
Configures auto negotiation advertisement of the duplex capability for a specified port or ports.

**Syntax**  
```plaintext
set port auto-negotiation-duplex-advertisement { <mod-num> | <mod-port-range> } [..., { <mod-num> | <mod-port-range> } ] { full/half-duplex | half-duplex }
```

**Sample Output**  
The following example sets the auto-negotiation advertisement of the duplex capability to full or half-duplex mode for the second fast ethernet port and ports 7 through 11 on the module in slot 5.

```
(configure) # set port auto-negotiation-duplex-advertisement 5/2,5/7-11 full/half duplex
Port auto-negotiation duplex advertisement set: 5/2,5/7,5/8,5/9,5/10,5/11
```

**Systems**  

**Table 21-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module where auto negotiation and advertisement of the duplex capability for every fast ethernet port on that module is set to support full or half duplex operations, or just half duplex operations.</td>
</tr>
<tr>
<td><code>&lt;mod-port-range&gt;</code></td>
<td>Specifies a range of fast ethernet port whose ability for auto negotiation and advertisement of their duplex capability is set to support full or half duplex operations or just half duplex operations.</td>
</tr>
<tr>
<td>{ full/half-duplex</td>
<td>Configure the duplex type of a port or range of ports.</td>
</tr>
<tr>
<td>half-duplex }</td>
<td>full/half duplex - Specifies that full- or half-duplex modes may be supported.</td>
</tr>
<tr>
<td></td>
<td>half-duplex - Specifies that half-duplex mode is the only mode supported.</td>
</tr>
</tbody>
</table>
set port auto-negotiation-flow-control-advertisement

Command Mode
Global Configuration.

Description
Sets the auto-negotiation flow control advertisement on a module or range of modules.

Syntax
set port auto-negotiation-flow-control-advertisement { <mod-num> | <mod-port-range> }

Sample Output
The following example sets the auto negotiation flow control advertisement of the module in slot 3.

(configure)# set port auto-negotiation-flow-control-advertisement 3

Systems

Table 21-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the auto negotiation and flow control advertisement is to be set.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Specifies a range of fast ethernet ports whose ability for auto negotiation and flow control advertisement to be set.
set port auto-negotiation-speed-advertisement

**Command Mode**  
Global Configuration.

**Description**  
Sets the auto-negotiation speed capability advertisement of fast ethernet ports to support speeds of 10Mbps, 100Mbps, or either.

**Syntax**  
```
set port auto-negotiation-speed-advertisement { <mod-num> | <mod-port-range> | ... | <mod-num> | <mod-port-range> } {10Mbps | 100Mbps | 10/100Mbps}
```

**Sample Output**  
The following example sets the auto negotiation advertisement of the speed capability to either 10 Mbps or 100 Mbps for the second fast ethernet port and ports 7 through 11 on the module in slot 5.

```
(configure)# set port auto-negotiation-speed-advertisement 5/2,5/7-11 10/100Mbps
Port auto-negotiation speed advertisement set: 5/2,5/7,5/8,5/9,5/10,5/11
```

**Systems**  

---

**Table 21-8. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module where the auto negotiation and advertisement of the speed capability for every fast ethernet port is set to support either 10Mbps or 100Mbps, or both.</td>
</tr>
<tr>
<td><code>&lt;mod-port-range&gt;</code></td>
<td>Specifies a range of fast ethernet ports whose ability for auto negotiation and advertisement of their speed capability is set to support either 10 Mbps, 100Mbps or both.</td>
</tr>
<tr>
<td>{10Mbps</td>
<td>100Mbps</td>
</tr>
</tbody>
</table>
set port auto-vlan-create

Command Mode  Global Configuration.

Description  Enables or disables auto VLAN creation for a specified switch port or all switch ports on a specified module. When enabled, it allows the switch to automatically create a VLAN each time the port receives a frame from an unknown VLAN.

Syntax

| To Enable: | set port auto-vlan-create \{ <mod-num> | <mod-swport-range> \}[,...,\{ <mod-num> | <mod-swport-range> \}] enable |
| To Disable: | set port auto-vlan-create \{ <mod-num> | <mod-swport-range> \}[,...,\{ <mod-num> | <mod-swport-range> \}] disable |

Table 21-9. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies a module number. If a module number is specified, auto-vlan-creation is set on all ports on the module</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a switch port or a range of switch ports on which to set the auto-vlan-create-parameter.</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables port auto-vlan-create.

```
(configure)# set port auto-vlan-create 4/1 enable
Port auto-vlan-create set: 4/1.
```

set port category

Command Mode  Global Configuration.

Description  Sets the category of ports.

Syntax  set port category {<mod-num> | <mod-port-range>} [...,{<mod-num> | <mod-port-range>}] {service-port | user-port}

Sample Output  The following example sets the category of all the ports on the module in slot 3 and ports 7 through 11 on the module in slot 5 as user ports.

```
(configure)# set port category 3,5/7-11 user-port
Port category set: 3/1,3/2,5/7,5/8,5/9,5/10,5/11
```

set port disable

**Command Mode**
Global Configuration.

**Description**
Disables a specified port or ports.

**Syntax**
```
set port disable {
    <mod-num>|
    <mod-port-range>
} [...,
    {<mod-num>|
    <mod-port-range>}] 
```

**Sample Output**
The following example disables all the ports on the module in slot 3 and ports 7 through 11 on the module in slot 5.

```
(configure)# set port disable 3,5/7-11
Port disable set: 3/1,3/2,5/7,5/8,5/9,5/10,5/11
```

**Systems**

---

### Table 21-11. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module where every port on that module is disabled.</td>
</tr>
<tr>
<td><code>&lt;mod-port-range&gt;</code></td>
<td>Specifies a range of ports to be disabled.</td>
</tr>
</tbody>
</table>
set port duplex

**Command Mode**
Global Configuration.

**Description**
Sets the duplexity of fast ethernet ports.

**Syntax**
```
set port duplex { <mod-num> | <mod-port-range> } [...., { <mod-num> | <mod-port-range> }] {full-duplex | half-duplex}
```

**Table 21-12. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the duplexity of every fast ethernet port is set.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies a range of fast ethernet ports whose duplexity is to be set.</td>
</tr>
<tr>
<td>{full-duplex</td>
<td>half-duplex}</td>
</tr>
<tr>
<td></td>
<td>• <strong>full duplex</strong> - The duplexity of the port is set to full duplex.</td>
</tr>
<tr>
<td></td>
<td>• <strong>half duplex</strong> - The duplexity of the port is set to half duplex.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets fast ethernet ports 7 through 11 on the module in slot 5 to full duplex mode.

```
(configure) # set port duplex 5/7-11 full-duplex
Port duplex mode set: 5/7,5/8,5/9,5/10,5/11
```

**Systems**
set port edge admin state

**Command Mode**
Global Configuration.

**Description**
Specifies whether a port is an edge port or a nonedge port. An edge port is not connected to any other bridge. Only edge ports and point-to-point links can rapidly transition to forwarding state.

If you set edge admin state to edge-port, the **OperEdgePort** field of the **show port** command is also set to edge-port. However, if the port receives a BPDU, the Oper Edge Port setting changes to non-edge-port. (To receive a BPDU, the port must be connected to a bridge and thus is not an edge port.)

**Syntax**
```
set port edge admin state <mod-swport-range>[,...,<mod-swport-range>]
{edge-port | non-edge-port}
```

**Table 21-13. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The module and port or port range.</td>
</tr>
<tr>
<td>edge-port</td>
<td>Defines the port as an edge port.</td>
</tr>
<tr>
<td>non-edge port</td>
<td>Defines the bridge as a nonedge port.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
set port enable

Command Mode  Global Configuration.

Description  Enables a specified port or ports.

Syntax  set port enable { <mod-num> | <mod-port-range> }[,...{ <mod-num> | <mod-port-range> }]

Sample Output  The following example enables all the ports on the module in slot 3 and ports 7 through 11 on the module in slot 5.

   (configure)# set port enable 3,5/7-11
   Port enable set: 3/1,3/2,5/7,5/8,5/9,5/10,5/11


Table 21-14. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where every port is enabled.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies a range of ports to be enabled.</td>
</tr>
</tbody>
</table>
set port flow-control

Command Mode
Global Configuration.

Description
Set the port flow control.

* Note: Setting this parameter on any M5548-100TX port sets all physical ports on the module to the same value.

Syntax
set port flow-control { <mod-num> | <mod-port-range> } [... { <mod-num> | <mod-port-range> }] { disable | enable | enable-receive-only | enable-send-only | enable-with-aggressive-backoff }

Sample Output
The following example sets the flow control on all the gigabit ports on the module in slot 3 to enable-receive-only.

```
(configure)# set port flow-control 3 enable-receive-only
Port flow control set: 3/1,3/2
```

Systems

### Table 21-15. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the flow control for each port on the module is to be set.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies the range of ports whose flow control is to be set.</td>
</tr>
</tbody>
</table>
| { disable | enable | enable-receive-only | enable-send-only | enable-with-aggressive-backoff} | The flow control options are:  
  - **disable** - Disables flow control for specified ports. Turns off an attached device's ability to send flow-control packets to a local port.  
  - **enable** - Enables flow control for specified ports. Turns on an attached device's ability to send flow-control packets to a local port.  
  - **enable-receive-only** - Enables receive only for the specified gigabit ports. Indicates that a port only receives administrative status from a remote device.  
  - **enable-send-only** - Enables send only for the specified gigabit ports. Indicates that a port only sends administrative status from a remote device.  
  - **enable-with-aggressive-backoff** - Enables flow control with aggressive backoff for specified fast ethernet ports. |
set port frame-tags

Command Mode  Global Configuration.

Description  Sets the switch ports to use or ignore frame tags.

Syntax  

```
set port frame-tags {<mod-num> | <mod-swport-range>} [..., {<mod-num> | <mod-swport-range>}] {ignore | use}
```

Command Mode  

The following example sets the second switch port on the module in slot 3 and switch ports 7 through 11 on the module in slot 5 to use frame tags.

```
(configure)# set port frame-tags 3/2, 5/7-11 use
Port frame-tags set: 3/2, 5/7, 5/8, 5/9, 5/10, 5/11
```

Systems  


### Table 21-16. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where every switch port on that module has the ability to use or ignore frame tag.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a range of switch ports that are able to use or ignore frame tags.</td>
</tr>
<tr>
<td>{ignore</td>
<td>use}</td>
</tr>
</tbody>
</table>
set port huntgroup

Command Mode Global Configuration.

Description Sets or clears the huntgroup assignment for a specified switch port.

Syntax

| To Configure: | set port huntgroup {<mod-num> | <mod-swport-range>}{...{<mod-num> | <mod-swport-range>}}<huntgroup-name> |
| To Clear:     | clear port huntgroup {<mod-num> | <mod-swport-range>}{...{<mod-num> | <mod-swport-range>}} |

Table 21-17. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module in chassis, which, if specified alone, sets or clears the huntgroup assignment of every switch port on the module.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a switch port or a range of switch ports whose hunt group assignments are set or cleared.</td>
</tr>
<tr>
<td>&lt;huntgroup-name&gt;</td>
<td>Specifies the name of a defined huntgroup.</td>
</tr>
</tbody>
</table>

Sample Output

The following example sets the huntgroup assignment of switch port 1 on the module in slot 5 to huntgroup named sales.

```
(configure)# set port huntgroup 5/1 huntgroup_sales
Port huntgroup set: 5/1.
```

The following example clears the huntgroup assignments for all switch ports on the module in slot 3.

```
(configure)# clear port huntgroup 3
Port huntgroup cleared: 3/1,3/2.
```

set port internal-error-shutdown

Command Mode  
Global Configuration.

Description  
Sets switch ports to shutdown if their rate of internal errors exceeds the threshold setting. To set the threshold, use the `set-internal-error-threshold` command. For information on this and other IEDR commands, see Chapter 18, “NEDR and IEDR.”

Syntax

| To Enable: | set port internal-error-shutdown { <mod-num> | <mod-swport-spec> | all-ports } enable |
| To Disable: | set port internal-error-shutdown {{ <mod-num> | <mod-swport-spec> | | all-ports } disable |

Table 21-18. Parameters, Keywords, Argument

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| { <mod-num> | <mod-swport-spec> } | The slot number of the module, and, either port number, or range of port numbers. Enter the port ranges in the format `Px-Py`. For example:  
  - To specify port 1 on the module in slot 3, enter `3/1`.  
  - To specify ports 1 through 5 on the module in slot 3, enter `3/1-5`. |
| all-ports | Enables or disables IEDR on all ports on all modules in the switch. |

Sample Output

The following example enables IEDR on all ports on the module in slot 3.

```
(configure) # set port internal-error-shutdown 3 enable
```

Systems

set port intrusion-trap

**Command Mode**  
Global Configuration.

**Description**  
Enables or disables the switch port intrusion trap.

**Syntax**

| To Enable: | set port intrusion-trap {<mod-num> | <mod-swport-range>} [....{<mod-num> | <mod-swport-range>}] enable |
| To Disable: | set port intrusion-trap {<mod-num> | <mod-swport-range>} disable |

**Table 21-19. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where every switch port on that module has the ability to use or ignore frame tag.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a range of switch ports that are able to use or ignore frame tags.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example enables the switch port intrusion trap on module in slot 3.

```
(configure)# set port intrusion-trap 3
```

**Systems**  
set port intrusion-trap-timer

Command Mode  Global Configuration.

Description  Sets the time interval at which intrusion traps are generated. The default setting for the intrusion trap timer is 1800 seconds (30 minutes). The valid range for the timer is 60 to 1800 seconds.

Syntax  

```
set port intrusion-trap-timer \{<mod-num>|<mod-swport-range>\} 
[...\{<mod-num>|<mod-swport-range>\}]<intrusion-trap-timer-value>
```

Table 21-20. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a range of switch ports.</td>
</tr>
</tbody>
</table>
| <intrusion-trap-timer-value> | Time interval at which intrusion traps are generated.  
The default setting for the intrusion trap timer is 1800 seconds (30 minutes). The valid range for the timer is 60 to 1800 seconds. |

**set port known-mode**

**Command Mode**  
Global Configuration.

**Description**  
Enables or disables known mode for the specified switch port or ports.

**Syntax**

```
To Enable:  set port known-mode {<mod-num> | <mod-swport-range>} [... {<mod-num> | <mod-swport-range>}] enable

To Disable: set port known-mode {<mod-num> | <mod-swport-range>} [... {<mod-num> | <mod-swport-range>}] disable
```

**Table 21-21. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module where the known mode of every switch port is enabled or disabled.</td>
</tr>
<tr>
<td><code>&lt;mod-swport-range&gt;</code></td>
<td>Specifies a range of switch ports whose known mode is to be enabled or disabled.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example enables known mode for the second switch port on the module in slot 3 and switch ports 7 through 11 on the module in slot 5.

```
(configure)# set port known-mode 3/2,5/7-11 enable
Port known-mode set: 3/2, 5/7, 5/8, 5/9, 5/10, 5/11
```

**Systems**  
set port mirror

Command Mode  Global Configuration.

Description  Set up or remove a port mirror on a switch in Fabric mode 1.

Syntax

To Configure:  
```
set port mirror <mod-port-range> source-port <mod-port-range> mirror-port <mod-port-spec> sampling {always | disable | periodic} [max-packets-sec <max-packets-sec-value>] [piggyback-port <mod-port-spec>]
```

To Clear:  
```
clear port mirror <mod-port-range>
```

Table 21-22. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-port-range&gt;</code></td>
<td>Specifies a mirror port range. The first mod-port-range in the command string is the port mirror rule identifier. It should be the physical port range for the rules associated fabric port. The source-port mod-port-range is the single port or the complete physical port range for the fabric port under investigation.</td>
</tr>
<tr>
<td><code>&lt;mod-port-spec&gt;</code></td>
<td>Specifies a particular port.</td>
</tr>
<tr>
<td>mirror-port</td>
<td>Port from which you want to send the traffic. This port can be on another module in the switch.</td>
</tr>
<tr>
<td>piggyback-port</td>
<td>The port that is used for bidirectional port mirroring. The specified port is unavailable for other uses.</td>
</tr>
<tr>
<td>sampling</td>
<td>Specifies how source port traffic is to be sampled (always, disabled or periodic based on max-packets-sec).</td>
</tr>
<tr>
<td>max-packets-sec</td>
<td>The maximum number of packets per second that are served by the mirror port. Only used when sampling is set to periodic. Valid values are 0, and 52 to 1,000,000.</td>
</tr>
</tbody>
</table>

Note: Eighty-series modules do not support piggyback ports.

Note: To mirror inbound traffic only, select a source port and a mirror port, not a piggyback port.
Sample Output  The following example sets a port mirror sampling rule for a single source port that has 2 fabric ports.

```
(configure)# set port mirror 4/1-10 source-port 4/2 mirror-port 4/3 sampling always piggyback-port 4/4
Port mirroring rule configured.
```

set port mirror Fabric_mode2

Command Mode Global Configuration.

Description Set up or remove a port mirror on a switch in Fabric mode 2.

Syntax

| To Configure: | set port mirror Fabric_mode2 source-port <mod-port-range> mirror-port <mod-port-spec> channel <channel> direction {tx | rx | both | sa | da} sampling {always | disable | periodic} [sa <MAC-address>] [da <MAC-address>] [max-packets-sec <max-packets-sec-value>] |
| To Clear: | clear port mirror Fabric_mode2 channel <channel> |

Table 21-23. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Either the single port or the range of ports that you want to mirror. See Table 21-24 for the specific port ranges that you can mirror.</td>
</tr>
<tr>
<td>&lt;mod-port-spec&gt;</td>
<td>The port to which you want to mirror traffic. Both the source port and mirror port must either:</td>
</tr>
<tr>
<td></td>
<td>• Be on the same vlan and have the same vlan binding or</td>
</tr>
<tr>
<td></td>
<td>• Have vlan binding set to bind to all</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Avaya recommends that you mirror traffic to a port of the same speed or faster than the source port.</td>
</tr>
<tr>
<td>&lt;channel&gt;</td>
<td>The mirror channel that you want to use. Four channels are available. Enter a number from 1 to 4.</td>
</tr>
<tr>
<td>{tx</td>
<td>rx</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can mirror transmit traffic of only one source port to the mirror port. You cannot mirror transmit traffic of multiple source ports to one mirror port.</td>
</tr>
</tbody>
</table>

1 of 2
Table 21-23. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{always</td>
<td>disable</td>
</tr>
<tr>
<td>[sa &lt;MAC-address&gt;]</td>
<td>The source MAC address that you want to mirror traffic for. Use this option only if you entered sa for the direction of traffic.</td>
</tr>
<tr>
<td>[da &lt;MAC-address&gt;]</td>
<td>The destination MAC address that you want to mirror traffic for. Use this option only if you entered da for the direction of traffic.</td>
</tr>
<tr>
<td>&lt;max-packets-sec-value&gt;</td>
<td>The maximum number of packets per second that you want the mirror port to receive. Use this option only if you entered Periodic for the sampling frequency.</td>
</tr>
</tbody>
</table>

Table 21-24. Port Ranges for Fabric Mode 2 Port Mirroring

<table>
<thead>
<tr>
<th>Module</th>
<th>Port ranges that you can mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-port gigabit modules</td>
<td>• 1–2</td>
</tr>
<tr>
<td></td>
<td>• 3–4</td>
</tr>
<tr>
<td></td>
<td>• Any single port</td>
</tr>
<tr>
<td></td>
<td>You can mirror any four single ports simultaneously (one port per channel). However you cannot mirror a port range and a single port within that range simultaneously.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> You <em>can</em> mirror port 1 on channel 1, port 2 on channel 2, and port 3 on channel 3 simultaneously. However, you <em>cannot</em> mirror ports 1 through 2 on channel 1 and port 2 on channel 2 simultaneously.</td>
</tr>
</tbody>
</table>
### Table 21-24. Port Ranges for Fabric Mode 2 Port Mirroring

<table>
<thead>
<tr>
<th>Module</th>
<th>Port ranges that you can mirror</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-port gigabit modules</td>
<td>• 1–4</td>
</tr>
<tr>
<td></td>
<td>• 5–8</td>
</tr>
<tr>
<td></td>
<td>• Any single port</td>
</tr>
<tr>
<td></td>
<td>You can mirror any four single ports simultaneously (one port per channel). However you cannot mirror a port range and a single port within that range simultaneously.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> You can mirror port 1 on channel 1, port 2 on channel 2, and port 3 on channel 3 simultaneously. However, you cannot mirror ports 1 through 4 on channel 1 and port 2 on channel 2 simultaneously.</td>
</tr>
<tr>
<td>24-port 10/100 modules</td>
<td>• 1–12 — any 1 port or the entire range.</td>
</tr>
<tr>
<td></td>
<td>• 13–24 — any 1 port or the entire range.</td>
</tr>
<tr>
<td></td>
<td>If you mirror a single port, you can mirror only 1 port per range at a time.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> You can mirror port 1 on channel 1 and port 13 on channel 2 simultaneously. However, you cannot mirror port 1 on channel 1 and port 2 on channel 2 simultaneously.</td>
</tr>
<tr>
<td>48-port 10/100 modules</td>
<td>• 1–12 — any 1 port or the entire range.</td>
</tr>
<tr>
<td></td>
<td>• 13–24 — any 1 port or the entire range.</td>
</tr>
<tr>
<td></td>
<td>• 25–36 — any 1 port or the entire range.</td>
</tr>
<tr>
<td></td>
<td>• 36–48 — any 1 port or the entire range.</td>
</tr>
<tr>
<td></td>
<td>If you mirror a single port, you can mirror only 1 port per range at a time.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> You can mirror port 1 on channel 1 and port 13 on channel 2 simultaneously. However, you cannot mirror port 1 on channel 1 and port 2 on channel 2 simultaneously.</td>
</tr>
</tbody>
</table>
**set port name**

**Command Mode**  
Global Configuration.

**Description**  
Sets the name for a port. Omitting the `<port-name>` variable clears the port name.

**Syntax**  
set port name `<mod-port-spec>` [<port-name>]

**Table 21-25. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-port-spec&gt;</code></td>
<td>Specifies a particular port by its module and port numbers.</td>
</tr>
<tr>
<td><code>&lt;port-name&gt;</code></td>
<td>Specifies the name to be assigned to the port. If a port name is not specified, the name of the port is cleared.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the name of the second port on the module in slot 3.

```
(configure)# set port name 3/2 "Really fast port"
Port name set: 3/2
```

**Systems**  
set port network-error-detection

**Command Mode**
Global Configuration.

**Description**
Configure network error detection and recovery (NEDR) for a port or ports.

**Syntax**

| To Enable: | set port network-error-detection <mod-port-range> [action {notify | disable-port}] [rising-threshold <rising-threshold-value>] [falling-threshold <falling-threshold-value>] [interval <interval seconds>] |
|------------|-------------------------------------------------------------------------------------------------|
| To Disable: | network-error-detection { <mod-port-range> | all } action off |

**Table 21-26. Parameters, Keywords, Argument**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| <mod-port-range> | The slot number of the module, and, either port number, or range of port numbers. Enter the port ranges in the format Px-Py. For example:  
- To specify port 1 on the module in slot 3, enter 3/1.  
- To specify ports 1 through 5 on the module in slot 3, enter 3/1-5. |
| all | Disables NEDR on all ports on all modules in the switch.  
**all** can be used only with **off**. |
| action {notify | disable-port | off} | Action that NEDR performs when the rate of errors exceeds the threshold. The options are:  
- **notify** - Logs the event in the event log  
- **disable-port** - Disables the port and logs the event in the event log.  
**Note:** A port will be disabled if the rate of errors equals or exceeds the threshold. Make sure a redundant protocol is configured.  
- **off** - Disables NEDR on the port or ports that you specify.  
The default setting is **notify**. |
**Sample Output**

The following command sets NEDR on ports 1-5 on module 3.

```
(configure)# set port network-error-detection 3/1-5
```

**Systems**


---

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;rising-threshold value&gt;</code></td>
<td>The rising threshold. The number of CRC errors that triggers NEDR to log an event in the event log or disable the port. The default setting is 100 (minimum is 1; maximum is 65535). <strong>Note:</strong> If you set the rising threshold value and the falling threshold value close together, events may be logged more often if the Notify option is selected.</td>
</tr>
<tr>
<td><code>&lt;falling-threshold value&gt;</code></td>
<td>The falling threshold. After exceeding the rising threshold, NEDR does not log another event in the event log until the rate of CRC errors falls below the falling threshold and then exceeds the rising threshold again. The default setting is half the rising threshold value (minimum is 0; maximum is 65535). <strong>Note:</strong> If you set the rising threshold value and the falling threshold value close together, events may be logged more often if the Notify option is selected.</td>
</tr>
<tr>
<td><code>&lt;interval-seconds&gt;</code></td>
<td>How often NEDR checks the number of errors occurring against the thresholds. Enter a number of seconds. The default setting is 2 seconds (minimum is 1; maximum is 65535).</td>
</tr>
</tbody>
</table>
set port pace-priority-mode

**Command Mode**: Global Configuration.

**Description**: Enables or disables pace priority mode on a specified port or ports.

**Syntax**

| To Enable: | set port pace-priority-mode {<mod-num> | <mod-port-range>} [... {<mod-num> | <mod-port-range>}] enable |
| To Disable: | set port pace-priority-mode {<mod-num> | <mod-port-range>} [... {<mod-num> | <mod-port-range>}] disable |

**Table 21-27. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies a module number where pace priority mode is enabled or disabled for every port on the module.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies a range of ports where pace priority mode is enabled or disabled.</td>
</tr>
</tbody>
</table>

**Sample Output**: The following example enables the pace priority mode on all the ports on the module in slot 3 and ports 7 through 11 on the module in slot 5.

```
(configure)# set port pace-priority-mode 3,5/7-11 enable
Port pace priority enable set: 3/1,3/2,5/7,5/8, 5/9,5/10,5/11
```

set port point-to-point admin status

Command Mode  
Global Configuration.

Description  
Specifies whether a port is connected to a shared LAN segment or a point-to-point LAN segment. A point-to-point LAN segment is connected to exactly one other bridge (normally with a direct cable between them). Only point-to-point links and edge ports can rapidly transition to forwarding state.

If you set this field to Auto, the switch automatically detects whether the port is connected to a shared link or a point-to-point link. Ports operating in half duplex are set to non-point-to-point, and ports operating in full duplex are set to point-to-point. You can, however, manually set the type of link.

Syntax  
set port point-to-point admin status {<mod-num> | <mod-swaprange> } [...{<mod-num> | <mod-swaprange> }] {force-true | force-false | auto}

Table 21-28. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-swaprange&gt;</td>
<td>The module and port or port range.</td>
</tr>
<tr>
<td>force-true</td>
<td>Defines the port as connected to a point-to-point link.</td>
</tr>
<tr>
<td>force-false</td>
<td>Defines the port as connected to a shared LAN segment.</td>
</tr>
<tr>
<td>auto</td>
<td>Automatically detects whether the port is connected to a shared link or a point-to-point link. Ports operating in half duplex are set to non-point-to-point, and ports operating in full duplex are set to point-to-point. If you select this setting, the OperPointToPoint field of the show port command displays the link type that is detected.</td>
</tr>
</tbody>
</table>

Systems  
P580 and P882.
set port rate-limit-burst-size

**Command Mode**  
Global Configuration.

**Description**  
Sets the rate limit burst size for fast ethernet ports.

* **Note:** Setting this parameter on any M5548-100TX port sets all physical ports on the module to the same value.

**Syntax**  
```
set port rate-limit-burst-size {<mod-num> | <mod-port-range>} 
[...{<mod-num> | <mod-port-range>}] {1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048}
```

**Table 21-29. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module where the rate limit burst size for each fast ethernet port on the module is to be set.</td>
</tr>
<tr>
<td><code>&lt;mod-port-range&gt;</code></td>
<td>Specifies the range of fast ethernet where the rate limit burst size is to be set.</td>
</tr>
<tr>
<td>`{1</td>
<td>2</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the rate limit burst size for the second fast ethernet port and ports 7-11 on the module in slot 5 to 512.

```
(configure)# set port rate-limit-burst-size 5/2,5/7-11 512
Port rate limit burst size set: 5/2, 5/7, 5/8, 5/9, 5/10, 5/11
```

**Systems**  
set port rate-limit-mode

**Command Mode**  
Global Configuration.

**Description**  
Sets the rate limit mode for fast ethernet ports.

**Syntax**  
set port rate-limit-mode {<mod-num> | <mod-port-range>} [... {<mod-num> | <mod-port-range>}] {disable | enable | enable-include-known-multicasts}

### Table 21-30. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the rate limit mode for fast ethernet ports are to be set.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies a range of fast ethernet ports whose rate limit mode is to be set.</td>
</tr>
<tr>
<td>{disable</td>
<td>enable</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the rate limit mode for the second fast ethernet port and ports 7 through 11 on the module in slot 5.

```
(configure)# set port rate-limit-mode 5/2,5/7-11 enable
Port rate limit mode set: 5/2,5/7,5/8,5/9,5/10,5/11
```

**Systems**  
set port rate-limit-rate

Command Mode
Global Configuration.

Description
Sets the rate limit rate for fast ethernet ports.

Syntax
```
set port rate-limit-rate { <mod-num> | <mod-port-range> } [..., { <mod-num> | <mod-port-range> } ] { 1% | 2% | 5% | 10% | 20% | 40% | 80% }
```

Sample Output
The following example sets the rate limit rate for the second fast ethernet port and ports 7 through 11 on the module in slot 5 to 80%.

```
(configure)# set port rate-limit-rate 5/2,5/7-11 80%
Port rate limit rate set: 5/2,5/7,5/8,5/9,5/10,5/11
```

Systems

**Table 21-31. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module where the rate limit rate for each fast ethernet port on the module is to be set.</td>
</tr>
<tr>
<td><code>&lt;mod-port-range&gt;</code></td>
<td>Specifies a port or a range of fast ethernet ports whose rate limit rate is to be set.</td>
</tr>
<tr>
<td>`{1%</td>
<td>2%</td>
</tr>
</tbody>
</table>
set port-redundancy

**Command Mode**  
Global Configuration.

**Description**  
Enables or disables all existing redundancy pairs.

**Syntax**  
set port-redundancy {enable | disable}

**Systems**  
P580 and P882.
set port-redundancy name

**Command Mode**
Global Configuration.

**Description**
Creates or deletes a port redundancy pair. After creating a redundancy pair, use the `set port-redundancy` command to enable port redundancy globally for all configured pairs.

*Note:* You must globally disable Spanning Tree and Rapid Spanning Tree before you can create a port redundancy pair.

**Syntax**

To Create:
```
set port-redundancy name <redundant-name>
<primary-port> <secondary-port>
```

To Delete:
```
no port-redundancy <redundant-name>
```

### Table 21-32. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;redundant-name&gt;</td>
<td>A unique name for the port redundancy pair.</td>
</tr>
<tr>
<td>&lt;primary-port&gt;</td>
<td>The primary port in the pair.</td>
</tr>
<tr>
<td>&lt;secondary-port&gt;</td>
<td>The secondary port in the pair.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
set port remote-fault-detect

**Command Mode**
Global Configuration.

**Description**
Enables or disables remote fault detections for gigabit ports. Remote fault detection makes it possible for a Gigabit port at one end of a link to signal status to the other end of the link, even if it does not have an operational receive link.

*Note:* Auto-negotiation and remote fault detection can not be enabled at the same time. Auto-negotiation must be disabled to enable remote fault detection. When auto-negotiation is enabled, remote fault detection is automatically disabled.

**Syntax**

| To Enable: | set port remote-fault-detect { <mod-num> | <mod-port-range> }[,...,{ <mod-num> | <mod-port-range> }] enable |
| To Disable: | set port remote-fault-detect { <mod-num> | <mod-port-range> }[,...,{ <mod-num> | <mod-port-range> }] disable |

**Table 21-33. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the ability to detect remote link errors for each gigabit port on the module is to be set.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies a port or a range of gigabit ports whose ability to detect remote link errors are enabled or disabled.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables remote fault detection in gigabit ports 1 and 2 on the module in slot 3 of an Avaya Multiservice switch.

```
(configure)# set port remote-fault-detect 3/1,3/2 enable
Port remote fault detection enable set: 3/1,3/2
```

**Systems**
set port spanning-tree-mode

**Command Mode**  
Global Configuration.

**Description**  
Enables or disables spanning tree mode for specified switch ports.

**Syntax**

| To Enable: | set port spanning-tree-mode {<mod-num> | <mod-swport-range>}[, <mod-num> | <mod-swport-range>] enable |
| To Disable: | set port spanning-tree-mode {<mod-num> | <mod-swport-range>}[, <mod-num> | <mod-swport-range>] disable |

**Table 21-34. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the spanning tree mode is to be enabled or disabled for every switch port on the module.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a range of switch ports whose spanning tree mode is to be enabled or disabled.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example enables the spanning tree mode for the second switch port on the module in slot 3 and switch port 7 through 11 on the module in slot 5 of an Avaya Multiservice Switch.

```
(configure)# set port spanning-tree-mode 3/2,5/7-11 enable
Port spanning-tree-mode set: 3/2,5/7,5/8,5/9, 5/10,5/11
```

**Systems**  
set port speed

Command Mode: Global Configuration.

Description: Sets the port speed.

Syntax:

```plaintext
set port speed { <mod-num> | <mod-port-range> }[...,{ <mod-num> | <mod-port-range> }] {10Mbps | 100Mbps | 1Gbps}
```

Sample Output:

```
The following example sets the speed for fast ethernet ports 7 through 11 on the module in slot 5 of an Avaya Multiservice switch to 100Mbps.

(configure)# set port speed 5/7-11 100Mbps
Port speed set: 5/7,5/8,5/9,5/10,5/11
```

set port trunking-format

**Command Mode**  
Global Configuration.

**Description**  
Sets the trunking format for switch ports. The default setting is clear.

**Syntax**  
```
set port trunking-format { <mod-num> | <mod-swport-range> } [..., { <mod-num> | <mod-swport-range> }] { clear | ieee-802.1Q | multi-layer | 3com }
```

**Table 21-36. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module where the trunking mode is to be set for each switch port on the module.</td>
</tr>
<tr>
<td><code>&lt;mod-swport-range&gt;</code></td>
<td>Specifies a range of switch ports whose trunking mode is to be set.</td>
</tr>
<tr>
<td>clear</td>
<td>Specifies the trunking option, which does no VLAN tagging.</td>
</tr>
<tr>
<td>ieee-802.1Q</td>
<td>Specifies the IEEE 802.1Q ethernet VLAN tagging trunking option.</td>
</tr>
<tr>
<td>multi-layer</td>
<td>Specifies a widely available proprietary VLAN tagging trunking option.</td>
</tr>
<tr>
<td>3com</td>
<td>Specifies the 3Com VLAN tagging trunking option.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the trunking option for the second switch port on the module in slot 3 and switch ports 7 through 11 on the module in slot 5 of an Avaya Multiservice switch to the IEEE standard.

```
(configure)# set port trunking-format 3/2,5/7-11 ieee-802.1Q
Port trunking-format set: 3/2,5/7,5/8,5/9,5/10,5/11
```

**Systems**  
**set port vlan**

**Command Mode**  
Global Configuration.

**Description**  
Sets the VLAN for a specified switch port or all switch ports on a specified module.

**Syntax**  
set port vlan {<mod-num> | <mod-swport-range> |,..., {<mod-num> | <mod-swport-range> } } <vlan-id>

**Table 21-37. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies a module number. If a module number is specified, the VLAN is set for all ports on the module.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a switch port or a range of switch ports where a VLAN is to be set.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The ID of the VLAN.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets a vlan on a specific port.

```
(configure)# set port vlan 3/1 1
Port VLAN set: 3/1
```

**Systems**  
set port vlan-binding-method

**Command Mode**  
Global Configuration.

**Description**  
Sets VLAN binding method for a specified switch port or all switch ports on a specified module.

**Syntax**  
set port vlan-binding-method {
  <mod-num> | <mod-swport-range>
} [...,
  <mod-num> | <mod-swport-range>
} {bind-to-all | bind-to-received | static}

**Table 21-38. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies a module number. If a module number is specified, the VLAN binding method is set for all ports on the module.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a switch port or a range of switch ports on which to set the VLAN binding method.</td>
</tr>
<tr>
<td>bind-to-all</td>
<td>Binds the port to all VLANs known to the switch.</td>
</tr>
<tr>
<td>bind-to-received</td>
<td>Binds this port to any VLAN it receives traffic from.</td>
</tr>
<tr>
<td>static</td>
<td>Assigns VLAN membership manually, using the VLAN switch ports.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example sets the VLAN binding to bind-to-all.

```
(configure)# set port vlan-binding-method 3/1 bind-to-all
Port vlan-binding-method set: 3/1
```

**Systems**  
set port vtp-snooping

**Command Mode**
Global Configuration.

**Description**
Disables or enables vtp-snooping for specified switch ports. The default state is disabled.

**Syntax**

| To Enable:      | set port vtp-snooping { <mod-num> | <mod-swport-range> }[,...{ <mod-num> | <mod-swport-range> }] enable |
|-----------------|--------------------------------------------------------------------------------------------------|
| To Disable:     | set port vtp-snooping { <mod-num> | <mod-swport-range> }[,...{ <mod-num> | <mod-swport-range> }] disable |

**Table 21-39. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>Specifies a particular port or a range of ports on a module.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables the vtp-snooping option for the second switch port on the module in slot 3 and switch ports 7 through 11 on the module in slot 5.

```
(configure)# set port vtp-snooping 3/2,5/7-11 enable
Port vtp-snooping set: 3/2,5/7,5/8,5/9,5/10,5/11
```

**Systems**
show port

Command Mode
User.

Description
Displays the configuration of specified switch ports. By default, the configuration of all switch ports is displayed.

Syntax
show port [{<mod-num>|<mod-swport-range>][..{<mod-num>|<mod-swport-range>}]}

Sample Output
The following example displays the configuration information of port 3 (partial).

> show port 3

<table>
<thead>
<tr>
<th>Port</th>
<th>Port VLAN (ID:Name)</th>
<th>Trunk Mode</th>
<th>VLAN Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>---------------------</td>
<td>------------</td>
<td>--------------</td>
</tr>
<tr>
<td>3/1</td>
<td>1:Default</td>
<td>clear</td>
<td>static</td>
</tr>
<tr>
<td>3/2</td>
<td>1:Default</td>
<td>clear</td>
<td>static</td>
</tr>
</tbody>
</table>

Systems
show port counters

**Command Mode**  
User.

**Description**  
Displays the port statistics on a module. If no `<mod-num>` or `<mod-swport-spec>` is specified, then the port statistics for all switch ports on all modules are displayed. If only a `<mod-num>` is specified, then port statistics for all switch ports on the specified module are displayed.

**Syntax**  
`show port counters [{<mod-num> | <mod-swport-spec>}]`

**Sample Output**  
The following example displays the ethernet interface statistics for port 1 of module 3.

```
> show port counters 3/1
Port 3/1
    Cleared: 02-Jan-18 14:01:31
    Receive Utilization:  0%
    Receive Bytes:       0
    Receive Unicast Packets: 0
    Receive Multicast Packets: 0
    Receive Discards:   0
    Receive Errors      54
    Transmit Utilization 0%
    Transmit Bytes     463,744
    Transmit Unicast Packets 0
```

**Systems**  

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies the number of the module in the chassis for which port statistics are to be displayed.</td>
</tr>
<tr>
<td><code>&lt;mod-swport-spec&gt;</code></td>
<td>Specifies a particular switch port whose specific port statistics are to be displayed.</td>
</tr>
</tbody>
</table>
**show port mirror**

**Command Mode**  
User.

**Description**  
Displays the port mirroring configuration for a specific source port or range or all source ports or ranges on a switch in Fabric mode 1. If no `<mod-num>` or `<mod-port-range>` is specified, then the port mirroring configuration of all switch ports is displayed. If a `<mod-num>` is specified, then all port mirroring sampling rules are displayed for the module.

**Syntax**

```
show port mirror [ [ <mod-num> | <mod-port-range> ] ]
```

**Table 21-42. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>Specifies a module number. If a module number is specified, all port mirroring rules on the module are displayed.</td>
</tr>
</tbody>
</table>
| `<mod-port-range>` | Specifies a particular port or a range of ports on a module.  
| **Note:**        | If no module numbers or module/port numbers are specified, all port mirror rules on the switch are displayed. |

**Sample Output**

The following example displays the port mirroring configuration information on the switch.

```
> show port mirror
Configure Source  Source Port  Mirror Port  Piggy Port  Sampler Type  Max Packets per Second
--------- ----- ----- ----- ---------- ----------
4/1-10 - - - -
4/11-20 4/11 4/12 4/13 always -
5/1 5/1 4/4 - periodic 200
```

**Systems**  
show port mirror Fabric_mode2

Command Mode  User.

Description  Displays the source ports, mirror port, direction being mirrored, MAC address filter, sampler type, and maximum packet per second for all port mirrors that are currently set up.

Syntax  show port mirror Fabric_mode2

Sample Output  The following example displays the port mirroring information on the Avaya Multiservice switch (partial).

```
> show port mirror Fabric_mode2
Channel    Source Port    Mirror Port    Direction/Filter    Sampler Type    Max Packets Per Second
----------    ---------    ----------    ------------------    ----------    --------------
1
2
3
4

Systems    P580 and P882.
```
show port physical

Command Mode  
User.

Description  
Displays the configuration of the specified physical port or ports.

Syntax  
show port physical [{<mod-num> | <mod-port-range>} [..., {<mod-num> | <mod-port-range> }]]

Table 21-43. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the configuration of every switch port is to be displayed.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies a range of ports on a module whose configuration is to be displayed.</td>
</tr>
</tbody>
</table>

Sample Output  
The following example displays the physical port configuration for the module in slot 6.

> show port physical 6

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>Category</th>
<th>Pace Priority</th>
<th>Mode</th>
<th>Remote Fault</th>
<th>Detect</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/1</td>
<td>Port 6/1</td>
<td>user-port</td>
<td>disable</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6/2</td>
<td>Port 6/2</td>
<td>user-port</td>
<td>disable</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6/3</td>
<td>Port 6/3</td>
<td>user-port</td>
<td>disable</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6/4</td>
<td>Port 6/4</td>
<td>user-port</td>
<td>disable</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>6/5</td>
<td>Port 6/5</td>
<td>user-port</td>
<td>disable</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Systems  
show port status

Command Mode  User.

Description  Displays port status information. The status information of all ports is displayed by default.

Syntax  show port status [{<mod-num>|<mod-port-range>} [...{<mod-num>|<mod-port-range>}]]

Sample Output  The following example displays the status of the ports on the modules in the switch.

> show port status
Port Type Mode StatusAutoNeg Speed Duplex
----- --------  --------  --------  -------------  ----------  -----------
3/1    Gigabit   Enabled   No Link   Disabled  1 Gb/s     Full Duplex
4/1    Gigabit   Enabled   No Link   Disabled  1 Gb/s     Full Duplex
4/2    Gigabit   Enabled   No Link   Disabled  1 Gb/s     Full Duplex
6/1    10/100    Enabled   No Link   Enabled   Auto-Neg   Auto-Neg
6/8    10/100    Enabled   No Link   Enabled   Auto-Neg   Auto-Neg
6/17   10/100    Enabled   No Link   Enabled   Auto-Neg   Auto-Neg


Table 21-44. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>Specifies the number of the module where the status of every port on that module is displayed.</td>
</tr>
<tr>
<td>&lt;mod-port-range&gt;</td>
<td>Specifies a range of ports whose status information is to be displayed.</td>
</tr>
</tbody>
</table>
show port redundancy

**Command Mode**  
User.

**Description**  
Displays the global port redundancy setting, enabled or disabled, and the configured redundancy pairs.

**Syntax**  
show port-redundancy [ <redundant-name> ]

---

**Table 21-45. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;redundant-name&gt;</td>
<td>The redundancy pair for which you want to view the configuration.</td>
</tr>
</tbody>
</table>

**Systems**  
P580 and P882.
22  Power Cool RAM

Overview

This chapter describes the following commands:

- `show system fans`
- `show system power`
- `show system ram`
show system fans

**Command Mode**  User.

**Description**  Displays the status of the cooling system.

**Syntax**  show system fans

**Sample Output**  The following example lists the status of the switch fans.

```
> show system fans
FanStatus
Module Fan Pair 1   Operational
Module Fan Pair 2   Operational
Fabric Fan 1        Operational
Fabric Fan 2        Operational
```

show system power

Command Mode
User.

Description
Displays the status of the power supplies installed in the chassis.

Syntax
show system power

Sample Output
The following example displays the status of the power supplies installed in the chassis.

> show system power
Power Supply Status Type
1 Present Power 1 SP627
2 Present Power 1 SP627
3 Present Power 1 SP627

Total System Power 600 Watts
Current Power Available 355 Watts

Systems
show system ram

Command Mode        User.

Description         Displays the status of Random Access Memory (RAM).

Syntax              show system ram

Sample Output       The following example displays the RAM status.

> show system ram
  Total RAM    64.00 MBytes
  Operational Image 5.80 MBytes

  Dynamically Allocated Memory
    Used       4.89 MBytes
    Max Used   5.90 MBytes
    Available  53.31 MBytes

  Allocation Failures 0

  System RAM Trap
    High Water Mark 57.60 MBytes

Overview

This chapter describes the following commands:

- access-list
- reset port queue counters
- set aft entry
- set diffserv plp
- set diffserv priority
- set port default-priority
- set port ignore-tag-priority
- set port mask-diffserv
- set port police
- set port queue service cbq
- set port queue service cbwfq
- set port queue service strict-priority
- set port queue service wfq
- set port use-diffserv
- show diffserv table
- show port
- show port police
- show port queue buffer
- show port queue counters
- show port queue service

*Important:* The QoS features are supported only on 80-series modules. 50-Series modules do not support these features.
access-list

Command Mode

Global Configuration.

Description

Creates a rule in an access control list (ACL). The rule that you set is applied on all of the ports on the switch.

* Note: You must enable the ACL on which you want to set a rule. Only one ACL can be enabled at a time.

The no command deletes an ACL rule or ACL.

Syntax

<table>
<thead>
<tr>
<th>To Create a Standard ACL Rule:</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list &lt;access-list-name&gt; &lt;access-list-index&gt;</td>
</tr>
<tr>
<td>{ permit [{ use-priority &lt;priority&gt;</td>
</tr>
<tr>
<td>remark-diffserv &lt;dscp&gt; [mask]</td>
</tr>
<tr>
<td>fwd2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To Create an Extended ACL Rule:</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list &lt;access-list-name&gt; &lt;access-list-index&gt;</td>
</tr>
<tr>
<td>{ permit [{ use-priority &lt;priority&gt;</td>
</tr>
<tr>
<td>fwd2</td>
</tr>
<tr>
<td>any</td>
</tr>
<tr>
<td>range &lt;port&gt; &lt;port&gt; } ] { &lt;dest-ip-addr&gt; &lt;dest-wildcard&gt;</td>
</tr>
<tr>
<td>gt &lt;port&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To Remove an ACL Rule or ACL:</th>
</tr>
</thead>
<tbody>
<tr>
<td>no access-list &lt;access-list-name&gt; [&lt;access-list-index&gt;]</td>
</tr>
</tbody>
</table>

Table 23-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;access-list-name&gt;</td>
<td>A unique name that identifies the access control list.</td>
</tr>
<tr>
<td>&lt;access-list-index&gt;</td>
<td>The unique rule number within the access list.</td>
</tr>
</tbody>
</table>
### Table 23-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>Forwards the packet without changing its priority.</td>
</tr>
<tr>
<td>use-priority</td>
<td>Assigns the priority that you define in the following <code>&lt;priority&gt;</code> parameter to the packet.</td>
</tr>
<tr>
<td><code>&lt;priority&gt;</code></td>
<td>The priority that you want to assign to packets that match this ACL. Enter a number between 0 and 7.</td>
</tr>
<tr>
<td>use-diffserv</td>
<td>Classifies traffic by the DSCP in the packet.</td>
</tr>
<tr>
<td>[mask]</td>
<td>Masks the three least significant bits of the DSCP.</td>
</tr>
<tr>
<td></td>
<td>If you mask the three least significant bits of the DSCP, the switch recognizes the remaining bits as the precedence field of the type of service (TOS) field and classifies the packets accordingly.</td>
</tr>
<tr>
<td>remark-diffserv</td>
<td>Replaces the DSCP in the packet with the DSCP that you enter for the following <code>&lt;dscp&gt;</code> parameter.</td>
</tr>
<tr>
<td></td>
<td>The switch uses the DSCP that you enter for the <code>&lt;dscp&gt;</code> parameter to classify the packet.</td>
</tr>
<tr>
<td><code>&lt;dscp&gt;</code></td>
<td>The DSCP that you want to replace the DSCP of the packet.</td>
</tr>
<tr>
<td>use-l2</td>
<td>Classifies traffic by the layer 2 priority of the packet. If you enter <code>use-l2</code>, the switch ignores the ACL rule priority and DiffServ priority.</td>
</tr>
<tr>
<td>deny</td>
<td>Blocks the packet.</td>
</tr>
<tr>
<td>fwd1</td>
<td>fwd2</td>
</tr>
<tr>
<td></td>
<td>The number following the <code>fwd</code> specifies the priority. The <code>fwdx</code> arguments are 1-based, while the queue priorities are 0-based. Consequently, the 1-based priorities are converted to 0-based priorities by the QoS features. For example, to specify a priority of 0, enter <code>fwd1</code>.</td>
</tr>
<tr>
<td></td>
<td>These keywords are retained from earlier versions of software for backward compatibility. The <code>use-priority </code>&lt;priority&gt;` keyword and argument serve the same function.</td>
</tr>
</tbody>
</table>
Table 23-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;protocol-id&gt;</td>
<td>The ID of the protocol that you want to assign a priority to. RFC791 defines the protocol IDs.</td>
</tr>
<tr>
<td>&lt;source-ip-addr&gt;</td>
<td>The source IP address of the subnet that you want to assign a priority to.</td>
</tr>
<tr>
<td>&lt;source-wildcard&gt;</td>
<td>The inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask. This parameter specifies a range of IP address. For example, to specify all IP addresses in the 10.10.70 subnet, enter <strong>10.10.70.0 0.0.0.255</strong>.</td>
</tr>
<tr>
<td>any</td>
<td>A source of 0.0.0.0 and a source-wildcard of 255.255.255.255</td>
</tr>
<tr>
<td>host &lt;source-ip-addr&gt;</td>
<td>The source IP address that you want to assign a priority to.</td>
</tr>
<tr>
<td>[{lt &lt;port&gt;</td>
<td>eq &lt;port&gt;</td>
</tr>
<tr>
<td>&lt;dest-ip-addr&gt;</td>
<td>The destination IP address of the subnet that you want to assign a priority to.</td>
</tr>
<tr>
<td>&lt;dest-wildcard&gt;</td>
<td>The inverse of a network mask. Enter a 32-bit number in four-part, dotted decimal format. Place ones in the bit positions that you want to mask. This parameter specifies a range of IP address. For example, to specify all IP addresses in the 10.10.70 subnet, enter <strong>10.10.70.0 0.0.0.255</strong>.</td>
</tr>
<tr>
<td>any</td>
<td>A destination of 0.0.0.0 and a destination-wildcard of 255.255.255.255</td>
</tr>
<tr>
<td>host &lt;dest-ip-addr&gt;</td>
<td>The destination IP address that you want to assign a priority to.</td>
</tr>
</tbody>
</table>
### Table 23-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[[lt &lt;port&gt;</td>
<td>eq &lt;port&gt;</td>
</tr>
<tr>
<td>[established]</td>
<td>Permits TCP connections to be established that match the rule.</td>
</tr>
</tbody>
</table>

---

### Sample Output: Standard ACL Rules

The following table provides examples of standard ACL rules.

### Table 23-2. Examples: Standard ACL Rules

<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use the DSCP in the packet to classify all traffic that has a source IP address in the 10.10.60 subnet. • Mask the three least significant bits of the DSCP.</td>
<td>(configure)# access-list MyAccessList1 4 permit use-diffserv mask 10.10.60.0 0.0.0.255</td>
</tr>
<tr>
<td>Assign a priority of 7 to all traffic that has a source IP address in the 10.10.70 subnet.</td>
<td>(configure)# access-list MyAccessList1 5 permit use-priority 7 10.10.70.0 0.0.0.255</td>
</tr>
<tr>
<td>• Replace the existing DSCP with a DSCP of 5 for all traffic that has a source IP address in the 10.10.80 subnet. • Mask the three least significant bits of the DSCP</td>
<td>(configure)# access-list MyAccessList1 6 permit remark-diffserv 5 mask 10.10.80.0 0.0.0.255</td>
</tr>
<tr>
<td>Use the layer 2 priority of the packet to classify all traffic that has a source address in the 11.11.11 subnet</td>
<td>(configure)# access-list MyAccessList1 7 permit use-l2 11.11.11.0 0.0.0.255</td>
</tr>
<tr>
<td>Use the DSCP in the packet to classify all traffic that has a source IP address of 199.93.239.168</td>
<td>(configure)# access-list MyAccessList1 8 permit use-diffserv host 199.93.239.168</td>
</tr>
</tbody>
</table>
**Table 23-2. Examples: Standard ACL Rules**

<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the DSCP in the packet to classify all traffic that has a source IP address of 3.3.3.3</td>
<td>(configure)# access-list MyAccessList1 9 permit use-diffserv mask host 3.3.3.3</td>
</tr>
<tr>
<td>Mask the three least significant bits of the DSCP</td>
<td></td>
</tr>
<tr>
<td>Assign a priority of 2 to all traffic that has a source IP address of 1.1.1.1</td>
<td>(configure)# access-list MyAccessList1 10 permit use-priority 2 1.1.1.1</td>
</tr>
<tr>
<td>Block all traffic that has a source IP address of 10.1.0.55</td>
<td>(configure)# access-list MyAccessList1 11 deny 10.1.0.55</td>
</tr>
</tbody>
</table>

**Sample Output:**

Extended ACL Rules

The following table provides examples of extended ACL rules.

**Table 23-3. Examples: Extended ACL Rules**

<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the DSCP in the packet to classify all traffic that has a:</td>
<td>(configure)# access-list MyAccessList2 1 permit use-diffserv ip host 199.93.239.168 1.1.1.0 0.0.0.255</td>
</tr>
<tr>
<td>• Source IP address of 199.93.239.168</td>
<td></td>
</tr>
<tr>
<td>• Destination address in the 1.1.1 subnet</td>
<td></td>
</tr>
<tr>
<td>Use the DSCP in the packet to classify all traffic that has a:</td>
<td>(configure)# access-list MyAccessList2 2 permit use-diffserv mask ip 3.0.0.0 0.255.255.255 5.0.0.0 0.255.255.255</td>
</tr>
<tr>
<td>• Source IP address in the 3.0 subnet</td>
<td></td>
</tr>
<tr>
<td>• Destination address in the 5.0 subnet</td>
<td></td>
</tr>
<tr>
<td>• Mask the three least significant bits of the DSCP</td>
<td></td>
</tr>
<tr>
<td>Assign a priority of 2 to all TCP traffic that has a:</td>
<td>(configure)# access-list MyAccessList2 3 permit use-priority 2 tcp 1.1.0.0 0.0.255.255 gt 24 6.6.0.0 0.0.255.255 eq 23</td>
</tr>
<tr>
<td>• Source IP address in the 1.1 subnet</td>
<td></td>
</tr>
<tr>
<td>• Source port that is greater than 24</td>
<td></td>
</tr>
<tr>
<td>• Destination IP address in the 6.6 subnet</td>
<td></td>
</tr>
<tr>
<td>• Destination port of 23</td>
<td></td>
</tr>
</tbody>
</table>
### Table 23-3. Examples: Extended ACL Rules

<table>
<thead>
<tr>
<th>To...</th>
<th>Enter...</th>
</tr>
</thead>
</table>
| • Replace the existing DSCP of packets with a DSCP of 12 for all traffic that has a source IP address of 199.93.238.83.  
• Mask the three least significant bits of the DSCP. | (configure)# access-list MyAccessList2 4 permit remark 12 mask ip host 199.93.238.83 any |
| Replace the existing DSCP of the packet with a DSCP of 24 for all ICMP traffic that has a:  
• Source IP address of 2.2.2.2  
• Destination IP address of 4.4.4.4 | (configure)# access-list MyAccessList2 5 permit remark 24 icmp host 2.2.2.2 host 4.4.4.4 |
| Assign a priority of 6 to all TCP traffic that has a:  
• Source IP address in the 10.10.10 subnet  
• Destination IP address in the 11.11.11 subnet  
• Destination port of 1 | (configure)# access-list MyAccessList2 6 permit use-priority 6 tcp 10.10.10.0 0.0.0.255 11.11.11.0 0.0.0.255 eq 1 |
| Use the layer 2 priority in the packet to classify all UDP traffic | (configure)# access-list MyAccessList2 7 permit use-l2 udp any any |
| • Use the layer 2 priority in the packet to classify all TCP traffic that has a:  
  — Source IP address in the 5.5.5 subnet  
  — Destination IP address in the 6.6.6 subnet  
  — Destination port that is less than 2  
• Permit TCP connections that meet this criteria | (configure)# access-list MyAccessList2 8 permit use-l2 tcp 5.5.5.0 0.0.0.255 6.6.6.0 0.0.0.255 lt 2 established |
### Table 23-3. Examples: Extended ACL Rules

<table>
<thead>
<tr>
<th>To...</th>
<th>Enter...</th>
</tr>
</thead>
</table>
| • Use the DSCP to classify all UDP traffic that has a:  
  — Source IP address of 7.7.7.7  
  — Destination IP address of 8.8.8.8  
  — Destination port between 33 and 44  
• Mask the three least significant bits of the DSCP  | (configure)# access-list MyAccessList2 9 permit use-diffserv mask udp host 7.7.7.7 host 8.8.8.8 range 33 44 |
| • Assign a priority of 7 to all TCP traffic that has a:  
  — Source IP address of 9.9.9.9  
  — Destination IP address of 3.3.3.3  
  — Destination port between 55 and 66  
• Permit TCP connections that meet this criteria | (configure)# access-list MyAccessList2 10 permit use-priority 7 tcp host 9.9.9.9 host 3.3.3.3 range 55 66 established |

### Systems
- P550R and P880, 80-series modules only.
- P580 and P882.
reset port queue counters

Command Mode
User.

Description
Resets the queue statistics to 0.

Syntax
reset port queue counters {<mod-num> | <mod-swport-range>}[...,
{<mod-num> | <mod-swport-range}>] {ingress | egress | all} [queue <queue>]

Table 23-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, the switch resets the QoS statistics for all ports on the module that you specify.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
  - To specify port 1 on the module in slot 3, enter 3/1.  
  - To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
  If you specify <mod-swport-range>, the switch resets the QoS statistics for the port or range of ports that you specify. |
| {ingress | egress | all} | The direction of traffic that you want to reset the QoS statistics for.  
  - Enter ingress to view the QoS statistics for ingress queues.  
  - Enter egress to view the QoS statistics for egress queues.  
  - Enter all to view the QoS statistics for both ingress and egress queues. |
| <queue>          | The queue number, which can range from 0 to 7. If you do not specify a queue number, the switch resets the QoS statistics for all queues on the port. |
Sample Output

The following example resets the QoS statistics on the ingress ports on the module in slot 3.

> reset port queue counters 3 ingress

Systems

- P550R and P880, 80-series modules only.
- P580 and P882.
set aft entry

Command Mode

Global Configuration.

Description

Configures the priority of a source MAC address or destination MAC address. The no command deletes the Address Forwarding Table (AFT) entry for the source or destination MAC address.

Syntax

| To Configure:                                      | set aft entry <mac-address> vlan {<vlan-id> | name <vlan-name>} port-binding {filter [forward <mod-port-spec>] [persistence {ageout | permanent}] [priority {normal | high}] [sa-priority {port | aft <entry-priority> | max-port-aft <entry-priority>}] [da-priority {port | aft <entry-priority> | max-port-aft <entry-priority>}]}
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------
| To Delete:                                        | clear aft entry <mac-address> vlan {<vlan-id> | name <vlan-name>}

Table 23-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mac-address&gt;</td>
<td>The MAC address associated with this entry.</td>
</tr>
<tr>
<td>vlan</td>
<td>The keyword for per VLAN commands.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The numerical ID of a specific VLAN.</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The name of the VLAN.</td>
</tr>
<tr>
<td>name</td>
<td>The keyword for the VLAN name.</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The name of the VLAN.</td>
</tr>
<tr>
<td>port-binding</td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>• filter - AFT entries with a filter port binding are dropped when received.</td>
</tr>
<tr>
<td></td>
<td>• forward - The port from which the mac address is forwarded.</td>
</tr>
<tr>
<td></td>
<td>• mod-port-spec - Specifies a particular port.</td>
</tr>
<tr>
<td>persistence</td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>• ageout - The entry is aged as per-learned entries.</td>
</tr>
<tr>
<td></td>
<td>• permanent - The entry is not aged out.</td>
</tr>
</tbody>
</table>

1 of 2
### Table 23-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>Options include:</td>
</tr>
<tr>
<td></td>
<td>- <strong>normal</strong> - The AFT entry has normal priority.</td>
</tr>
<tr>
<td></td>
<td>- <strong>high</strong> - The AFT entry has high priority.</td>
</tr>
<tr>
<td>sa-priority port</td>
<td>Uses the priority of the physical port, Cisco ISL tag, or 802.1p tag to determine the layer 2 priority of frames.</td>
</tr>
<tr>
<td>sa-priority aft</td>
<td>Uses the priority that is assigned to the source MAC address in the Address Forwarding Table (AFT) to determine the layer 2 priority of frames.</td>
</tr>
<tr>
<td>&lt;entry-priority&gt;</td>
<td>The priority that you want to assign to the source MAC address. Enter a number between 0 and 7. This priority is stored in the AFT entry for the MAC address that you specify.</td>
</tr>
<tr>
<td>sa-priority max-port-aft</td>
<td>Determines the priority of a frame by using the higher of the:</td>
</tr>
<tr>
<td></td>
<td>- Physical port priority or tag priority</td>
</tr>
<tr>
<td></td>
<td>- Source MAC address priority</td>
</tr>
<tr>
<td>da-priority port</td>
<td>Uses the priority of the physical port, Cisco ISL tag, 802.1p tag, or source MAC address to determine the layer 2 priority of frames.</td>
</tr>
<tr>
<td>da-priority aft</td>
<td>Uses the priority that is assigned to the destination MAC address in the AFT to determine the priority of the frame.</td>
</tr>
<tr>
<td>&lt;entry-priority&gt;</td>
<td>The priority that you want to assign to the destination MAC address. Enter a number between 0 and 7.</td>
</tr>
<tr>
<td>da-priority max-port-aft</td>
<td>Determines the priority of the frame by using the higher of the:</td>
</tr>
<tr>
<td></td>
<td>- Physical port priority or tag priority</td>
</tr>
<tr>
<td></td>
<td>- Destination MAC address priority</td>
</tr>
</tbody>
</table>
The following table provides examples of this command.

### Table 23-6. Examples: set aft entry

<table>
<thead>
<tr>
<th>To...</th>
<th>Enter...</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50. • Forward frames that have a source or destination MAC address of 00:00:00:00:00:55. • Assign a priority of 7 to frames that have a source MAC address of 00:00:00:00:00:55.</td>
<td>(configure)# set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 sa-priority aft 7</td>
</tr>
<tr>
<td>• Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50. • Forward frames that have a source or destination MAC address of 00:00:00:00:00:55. • Assign a priority of 5 with the source MAC address of 0:00:00:00:00:55. • Assign the higher of the port priority, tag priority, or source MAC address priority (5) to frames that have a source MAC address of 00:00:00:00:00:55.</td>
<td>(configure)# set aft entry 00:00:00:00:00:55 VLAN 50 port-binding forward 3/1 sa-priority max-port-aft 5</td>
</tr>
</tbody>
</table>
### Table 23-6. Examples: set aft entry

<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.</td>
<td></td>
</tr>
<tr>
<td>• Forward frames that have a source or destination MAC address of 00:00:00:00:55.</td>
<td></td>
</tr>
<tr>
<td>• Assign a priority of 7 to packets that have a destination MAC address of 00:00:00:00:55.</td>
<td>(configure)# set aft entry 00:00:00:00:55 VLAN 50 port-binding forward 3/1 da-priority aft 7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>To . . .</th>
<th>Enter . . .</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Associate MAC address 00:00:00:00:00:55 with port 1 on the module in slot 3 and with VLAN 50.</td>
<td></td>
</tr>
<tr>
<td>• Forward frames that have a source or destination MAC address of 00:00:00:00:55.</td>
<td></td>
</tr>
<tr>
<td>• Associate a priority of 5 with the destination MAC of address 0:00:00:00:55.</td>
<td></td>
</tr>
<tr>
<td>• Assign the higher of the port priority, tag priority, or destination MAC address priority (5) to frames that have a destination MAC address of 00:00:00:00:55.</td>
<td>(configure)# set aft entry 00:00:00:00:55 VLAN 50 port-binding forward 3/1 da-priority max-port-aft 5</td>
</tr>
</tbody>
</table>

---

**Systems**

- P550R and P880, 80-series modules only.
- P580 and P882.
set diffserv plp

* **Important:** This command is for future functionality and is not currently supported.

**Command Mode**
Global Configuration.

**Description**
Assigns a packet loss probability (PLP) to a DiffServ code point (DSCP).

**Syntax**
```
set diffserv plp {low | high} dscp <dscp-start-range> [<dscp-end-range>]
```

**Table 23-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{low</td>
<td>high}</td>
</tr>
<tr>
<td><code>&lt;dscp-start-range&gt;</code></td>
<td>The first DSCP in the range of DSCPs that you want to assign the PLP to. DSCPs range from 0 to 63.</td>
</tr>
<tr>
<td>[&lt;dscp-end-range&gt;]</td>
<td>The last DSCP in the range of DSCPs that you want to assign the PLP to. DSCPs range from 0 to 63.</td>
</tr>
</tbody>
</table>

* **Note:** While the PLP for a DSCP can be configured and displayed, the PLP is applied only when RED is enabled on a port.

**Systems**
- P550R and P880, 80-series modules only.
- P580 and P882.
set diffserv priority

Command Mode  
Global Configuration.

Description  
Assigns a priority to a DiffServ code point (DSCP) in the DiffServ Mapping Table.

Syntax  
set diffserv priority <priority> dscp <dscp-start-range> [<dscp-end-range>]

Table 23-8. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;priority&gt;</td>
<td>The priority that you want to assign. Enter a number between 0 and 7.</td>
</tr>
<tr>
<td>&lt;dscp-start-range&gt;</td>
<td>The first DSCP in the range of DSCPs that you want to assign the priority to. DSCPs range from 0 to 63.</td>
</tr>
<tr>
<td>[&lt;dscp-end-range&gt;]</td>
<td>The last DSCP in the range of DSCPs that you want to assign the priority to. DSCPs range from 0 to 63.</td>
</tr>
</tbody>
</table>

Sample Output  
The following command sets a priority of 7 to DSCPs 15 through 63.

(configure)# set diffserv priority 7 dscp 15 63

Systems  
- P550R and P880, 80-series modules only.
- P580 and P882.
set port default-priority

**Command Mode**
Global Configuration.

**Description**
Sets the priority of a physical port.

**Syntax**
`set port default-priority [{<mod-num> | <mod-swport-range>}][..., {<mod-num> | <mod-swport-range>}] | all-ports} <priority>`

**Table 23-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>The slot number of a module. If you specify <code>&lt;mod-num&gt;</code>, the priority is set for all ports on the module.</td>
</tr>
<tr>
<td><code>&lt;mod-swport-range&gt;</code></td>
<td>The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:</td>
</tr>
<tr>
<td></td>
<td>• To specify port 1 on the module in slot 3, enter 3/1.</td>
</tr>
<tr>
<td></td>
<td>• To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.</td>
</tr>
<tr>
<td></td>
<td>If you specify <code>&lt;mod-swport-range&gt;</code>, the priority is set for the port or range of ports on the module that you specify.</td>
</tr>
<tr>
<td>all-ports</td>
<td>All ports in the chassis. If you specify all-ports, all ports on all modules in the chassis are set with the same priority.</td>
</tr>
<tr>
<td><code>&lt;priority&gt;</code></td>
<td>The priority that you want to assign to the port or port range. Enter a number between 0 and 7. The highest priority is 7.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command sets the priority to 0 for all ports on the module in slot 3.

```
(configure)# set port default-priority 3 0
```

The following command sets the priority to 5 for ports 1 through 5 on the module in slot 3.

```
(configure)# set port default-priority 3/1-5 5
```
The following command sets the priority to 2 for ports 1 through 5 on the module in slot 3 and for port 1 on the module in slot 6.

```
(configure)# set port default-priority 3/1-5,6/1 2
```

**Systems**

- P550R and P880, 80-series modules only.
- P580 and P882.
set port ignore-tag-priority

**Command Mode**  
Global Configuration.

**Description**  
Sets a port to ignore any layer 2 tag priority (including 802.1p tags). The default setting is off.

**Syntax**

| To Enable: | set port ignore-tag-priority {{ <mod-num> | <mod-swport-range> }[,...,{ <mod-num> | <mod-swport-range> }]} | all-ports} on |
|------------|-------------------------------------------------------------------------------------------------|
| To Disable:| set port ignore-tag-priority {{ <mod-num> | <mod-swport-range> }[,...,{ <mod-num> | <mod-swport-range> }]} | all-ports} off |

**Table 23-10. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, the switch ignores tag priorities on all ports of the module.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:</td>
</tr>
<tr>
<td></td>
<td>• To specify port 1 on the module in slot 3, enter 3/1.</td>
</tr>
<tr>
<td></td>
<td>• To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.</td>
</tr>
<tr>
<td></td>
<td>If you specify &lt;mod-swport-range&gt;, the switch ignores tag priorities on the port or range of ports on the module in the slot that you specify.</td>
</tr>
<tr>
<td>all-ports</td>
<td>All ports in the chassis. If you specify all-ports, all ports on all modules in the chassis are set with the same priority.</td>
</tr>
<tr>
<td>{on</td>
<td>off}</td>
</tr>
</tbody>
</table>
Sample Output

The following command sets all ports on the module in slot 3 to ignore the 802.1p tag priority

(configure)# set port ignore-tag-priority 3 on

The following command sets ports 1 through 5 on the module in slot 3 to not ignore the 802.1p tag priority

(configure)# set port ignore-tag-priority 3/1-5 off

The following command sets ports 1 through 5 on the module in slot 3 and port 1 on the module in slot 6 to ignore the 802.1p tag priority.

(configure)# set port ignore-tag-priority 3/1-5,6/1 on

Systems

- P550R and P880, 80-series modules only.
- P580 and P882.
set port mask-diffserv

Command Mode
Global Configuration.

Description
Sets a port to mask the three least significant bits of the DSCP when the switch is using the DSCP to classify bridged IP traffic. If you mask the three least significant bits of the DSCP, the switch recognizes the remaining bits as the precedence field of the Type of Service (ToS) field and classifies the packets accordingly.

Syntax

| To Enable: | set port mask-diffserv { { <mod-num> | <mod-swport-range> }[,..,{ <mod-num> | <mod-swport-range> }] | all-ports } on |
|------------|----------------------------------------------------------------------------------------------------------------------------------|
| To Disable:| set port mask-diffserv { { <mod-num> | <mod-swport-range> }[,..,{ <mod-num> | <mod-swport-range> }] | all-ports } off |

Table 23-11. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, all ports on the module mask the three least significant bits of the DSCP.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:</td>
</tr>
<tr>
<td></td>
<td>• To specify port 1 on the module in slot 3, enter 3/1.</td>
</tr>
<tr>
<td></td>
<td>• To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.</td>
</tr>
<tr>
<td></td>
<td>If you specify &lt;mod-swport-range&gt;, the port or range of ports on the module that you specify mask the three least significant bits of the DSCP.</td>
</tr>
</tbody>
</table>

1 of 2
Table 23-11. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{all-ports}</td>
<td>All ports in the chassis. If you enter all-ports, all ports in the chassis are set to mask the three least significant bits of the DSCP.</td>
</tr>
<tr>
<td>{on</td>
<td>off}</td>
</tr>
<tr>
<td></td>
<td>• Enter on to mask the bits.</td>
</tr>
<tr>
<td></td>
<td>• Enter off to not mask the bits.</td>
</tr>
</tbody>
</table>

Sample Output

The following command sets all ports on the module in slot 3 to mask the three least significant bits of the DSCP, enter:

(configure)# set port mask-diffserv 3 on

Systems

- P550R and P880, 80-series modules only.
- P580 and P882.
set port police

Command Mode  Global Configuration.

Description  Enables or disables policing for ingress traffic on a port.

Syntax

| To Configure: | set port police {{ <mod-num> | <mod-swport-range> } | all-ports} queue <queue> {bit-rate <rate> normal-burst <normal-burst>} |
| To Disable:    | set port police {{ <mod-num> | <mod-swport-range> } | all-ports} queue <queue> disable |

Table 23-12. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, policing is enabled for all ports on the module in the slot that you specify.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
  • To specify port 1 on the module in slot 3, enter 3/1.  
  • To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
  If you specify <mod-swport-range>, policing is enabled for the port or range of ports on the module in the slot that you specify. |
| all-ports       | All ports in the chassis. If you specify all-ports, policing is enabled on all modules in the chassis. |
| <queue>         | The queue number, which can range from 0 to 7.                             |
Sample Output

The following example sets port police on all ports on module 3.

(configure)# set port police 3 all-ports

Systems

- P550R and P880, 80-series modules only.
- P580 and P882.

---

**Table 23-12. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;rate&gt;</td>
<td>The maximum bits per second that you want to assign to the queue.</td>
</tr>
<tr>
<td></td>
<td>For Fabric mode 1, enter:</td>
</tr>
<tr>
<td></td>
<td>• 0 to disable the queue</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• 220 Kbps to 1.5 Gbps</td>
</tr>
<tr>
<td></td>
<td>For Fabric mode 2, enter:</td>
</tr>
<tr>
<td></td>
<td>• 0 to disable the queue</td>
</tr>
<tr>
<td></td>
<td>Or</td>
</tr>
<tr>
<td></td>
<td>• 270 Kbps to 1.5 Gbps</td>
</tr>
<tr>
<td>&lt;normal-burst&gt;</td>
<td>This threshold sets the maximum size of burst that is guaranteed transfer.</td>
</tr>
<tr>
<td></td>
<td>The normal burst can range from 0 to 15,000. Avaya recommends a setting of 4.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables policing.</td>
</tr>
</tbody>
</table>

2 of 2
set port queue service cbq

**Command Mode**  
Global Configuration.

**Description**  
Sets a port, port range, or module to use class-based queuing (CBQ) queue servicing.

**Syntax**  
set port queue service { [<mod-num>] | <mod-swport-range> }[...{ [<mod-num>] | <mod-swport-range> } | all-ports} cbq queue <queue> bit-rate <rate>

---

### Table 23-13. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, all ports on the module are set to use CBQ.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
                      - To specify port 1 on the module in slot 3, enter 3/1.  
                      - To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
                      If you specify <mod-swport-range>, the port or range of ports that you specify is set use CBQ. |
| all-ports          | All ports in the chassis. If you specify all-ports, all ports on all modules in the chassis are set to use CBQ.                             |
| <queue>            | The queue number, which can range from 0 to 7.                                                                                           |
| <rate>             | The maximum bits per second that you want to assign to the queue.  
                      If the switch is operating in Fabric mode 1, the rate can range from 220 Kbps to 1.5 Gbps.  
                      If the switch is operating in Fabric mode 2, the rate can range from 270 Kbps to 1.5 Gbps  
                      Entering a rate of 0 disables the queue.                                                                                           |

**Systems**  
- P550R and P880, 80-series modules only.
- P580 and P882.
set port queue service cbwfq

**Command Mode** Global Configuration.

**Description** Sets a port, port range, or module to use class-based weighted fair queuing (CBWFQ) queue servicing.

**Syntax**

```
set port queue service {{<mod-num> | <mod-swport-range>}[... {<mod-num> | <mod-swport-range>}]} | all-ports} cbwfq queue <queue> bit-rate <rate> normal-burst <normal-burst> [exceed {drop | max-burst <max-burst>} [weight <weight>]]
```

**Table 23-14. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, all ports on the module are set to use CBQ.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
  - To specify port 1 on the module in slot 3, enter 3/1.  
  - To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
  If you specify <mod-swport-range>, the port or range of ports that you specify is set use CBQ. |
| all-ports      | All ports in the chassis. If you specify all-ports, all ports on all modules in the chassis are set to use CBQ. |
| <queue>        | The queue number, which can range from 0 to 7.                               |
| <rate>         | The maximum bits per second that you want to assign to the queue.  
  If the switch is operating in Fabric mode 1, the rate can range from 220 Kbps to 1.5 Gbps.  
  If the switch is operating in Fabric mode 2, the rate can range from 270 Kbps to 1.5 Gbps  
  Entering a rate of 0 disables the queue. |

1 of 2
### Table 23-14. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;normal-burst&gt;</td>
<td>The maximum size of burst that is guaranteed transfer. Bursts that are smaller than this size are guaranteed transfer. Bursts that are larger than this size are either serviced by WFQ or dropped (whichever action that you specify). The default setting is servicing by WFQ and the default weight for the queues. The normal burst can range from 0 to 15,000 bytes. Avaya recommends a value of 6000. Enter this setting in a multiple of four. If you do not enter a multiple of four, the switch rounds down the number that you enter to a multiple of four. For example, if you enter a normal burst size of 43 bytes, the switch converts the setting to 40 bytes. If you enter a normal burst size of 0,1,2 or 3, the switch stores a value of 0 and no data is forwarded from the queue.</td>
</tr>
<tr>
<td>exceed</td>
<td>The action that you want the switch to take if the bit rate exceeds the guaranteed bit rate that you specify. The switch can either drop packets or forward them based on the weight of the queue.</td>
</tr>
<tr>
<td>drop</td>
<td>Indicates that you want the switch to drop packets when the bit rate exceeds the guaranteed bit rate.</td>
</tr>
<tr>
<td>&lt;max-burst&gt;</td>
<td>The maximum size burst that is serviced by WFQ once the normal burst has been exceeded. Bursts that are smaller than this size are serviced by WFQ. Bursts that are larger than this size are dropped. If you set this threshold to the same value as normal burst, the maximum burst capability is disabled. The maximum burst can range from the normal burst size to 15,000. Avaya recommends a value of 6000. Increase the maximum burst setting as the burstiness of the traffic increases. <strong>Note:</strong> The maximum burst setting must be greater than or equal to the normal burst. Enter this setting in a multiple of four. If you do not enter a multiple of four, the switch rounds down the number that you enter to a multiple of four. For example, if you enter a maximum burst size of 43 bytes, the switch converts the setting to 40 bytes. If you enter a maximum burst size of 0,1,2 or 3, the switch stores a value of 0 and no data is forwarded from the queue.</td>
</tr>
<tr>
<td>&lt;weight&gt;</td>
<td>The weight that you want to assign to the queue. Weights can range from 1 to 254.</td>
</tr>
</tbody>
</table>

**Systems**

- P550R and P880, 80-series modules only.
- P580 and P882.
**set port queue service strict-priority**

**Command Mode**
Global Configuration.

**Description**
Sets a port, port range, or module to use strict priority queue servicing.

**Syntax**
```
set port queue service [{<mod-num> | <mod-swport-range>}]....,{<mod-num> | <mod-swport-range>}] | all-ports} strict-priority
```

**Sample Output**
The following example set ports 1 through 12 on module 5 to use strict priority queueing.

```
(configure)# set port queue service 5/1-12 strict-priority
```

**Systems**
- P550R and P880, 80-series modules only.
- P580 and P882.

---

**Table 23-15. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, all ports on the module are set to use strict priority queueing.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
- To specify port 1 on the module in slot 3, enter 3/1.  
- To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
  If you specify <mod-swport-range>, the port or range of ports on the module that you specify is set to use strict priority queueing. |
| all-ports        | All ports in the chassis. If you specify all-ports, all ports on all modules in the chassis are set to use strict priority queueing. |
set port queue service wfq

Command Mode
Global Configuration.

Description
Sets a port, port range, or module to use weighted fair queueing (WFQ) queue servicing. WFQ is the default queue-servicing algorithm.

Syntax
set port queue service {{ <mod-num> | <mod-swport-range> } [...,{ <mod-num> | <mod-swport-range> }]} all-ports} wfq {queue <queue> weight <weight> | default}

Table 23-16. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, all ports on the module are set to use WFQ.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format P<sup>x</sup>-P<sup>y</sup>. For example:  
  - To specify port 1 on the module in slot 3, enter 3/1.  
  - To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
  If you specify <mod-swport-range>, the port or range of ports that you specify is set to use WFQ. |
| all-ports       | All ports in the chassis. If you specify all-ports, all ports on all modules in the chassis are set to use WFQ. |
| <queue>         | The queue number, which can range from 0 to 7. |
| <weight>        | The weight that you want to assign to the queue. Weights can range from 1 to 254. |
| default         | The default weights. |

Systems
- P550R and P880, 80-series modules only.
- P580 and P882.
set port use-diffserv

Command Mode
Global Configuration.

Description
Sets a port to classify bridged IP traffic by its DiffServ code point (DSCP).

Syntax

| To Enable: | set port use-diffserv { {{<mod-num>} | <mod-swport-range>} | ... | {{<mod-num>} | <mod-swport-range>} } | all-ports } on |
| To Disable: | set port use-diffserv { {{<mod-num>} | <mod-swport-range>} | ... | {{<mod-num>} | <mod-swport-range>} } | all-ports } off |

Table 23-17. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, the switch ignores tag priorities on all ports of the module.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
  • To specify port 1 on the module in slot 3, enter 3/1.  
  • To specify ports 1 through 5 on the module in slot 3, enter 3/1-5. If you specify <mod-swport-range>, the switch ignores tag priorities on the port or range of ports on the module in the slot that you specify. |
| all-ports          | All ports in the chassis. If you specify all-ports, all ports on all modules in the chassis are set with the same priority. |
| {on | off}            | Indicates whether you want the port to ignore tag priority. Enter on for the port to ignore the tag priority. |
Sample Output

The following command sets ports 4 through 12 on the module in slot 6 to classify bridged IP traffic by DSCP:

(configure)# set port use-diffserv 6/4-12 on

Systems

- P550R and P880, 80-series modules only.
- P580 and P882.
## show diffserv table

**Command Mode**  
User.

**Description**  
Display the priority that is assigned to each DSCP.

* **Note:** The `show diffserv table` CLI command displays the packet loss probability (PLP) for each DSCP. However, the switch does not currently support PLP.

**Syntax**  
```
show diffserv table
```

**Sample Output**  
The following example displays the diffserv table.

```
> show diffserv table
```

**Systems**  
- P550R and P880, 80-series modules only.
- P580 and P882.
show port

Command Mode  User.

Description  Displays the QoS settings for a physical port. This command also displays the priority of the port, if the port is set to ignore 802.1p tag priority, and if the port is set to use the DSCP for bridged IP traffic.

Syntax  show port [{<mod-num> | <mod-swport-range>}...{<mod-num> | <mod-swport-range>}]]

Table 23-18. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, the switch displays the QoS settings for all ports on the module in the slot that you specify.</td>
</tr>
</tbody>
</table>
| <mod-swport-range>    | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
  • To specify port 1 on the module in slot 3, enter 3/1.  
  • To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
  If you specify <mod-swport-range>, the switch displays the QoS settings for the port or range of ports on the module in the slot that you specify. |

Sample Output  The following example displays the QoS settings for module 3.

  > show port 3

Systems  
  ■ P550R and P880, 80-series modules only.  
  ■ P580 and P882.
show port police

Command Mode
User.

Description
Displays the settings for policing.

Syntax
show port police { <mod-num> | <mod-swport-range> } [...] { <mod-num> | <mod-swport-range> }

Table 23-19. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, the switch displays the policing settings for all ports on the module in the slot that you specify.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
  • To specify port 1 on the module in slot 3, enter 3/1.  
  • To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
  If you specify <mod-swport-range>, the switch displays the policing settings for the port or range of ports on the module in the slot that you specify. |

Sample Output
The following example displays the policing settings for all ports on module 3.

> show port police 3

Systems
- P550R and P880, 80-series modules only.
- P580 and P882.
show port queue buffer

**Command Mode** User.

**Description** Displays the amount of memory that is assigned to each queue.

**Syntax**

```
show port queue buffer {{<mod-num> | <mod-swport-range>} [..., {<mod-num> | <mod-swport-range>}]} | all-ports}
```

**Sample Output**

The following example displays the amount of memory that is assigned to all ports on the module in slot 3.

```
> show port queue buffer 3 all-ports
```

**Systems**

- P550R and P880, 80-series modules only.
- P580 and P882.

---

**Table 23-20. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. The switch displays the number of packet buffers that are allocated to the egress queues on all ports on the module that you specify.</td>
</tr>
</tbody>
</table>
| <mod-swport-range>    | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
                        | • To specify port 1 on the module in slot 3, enter 3/1.  
                        | • To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
                        | The switch displays the number of packet buffers that are allocated to the egress queues on the port or range of ports that you specify. |
| {all-ports}           | All ports in the chassis. The switch displays the number of packet buffers that are allocated to the egress queues on all ports in the chassis. |
show port queue counters

Command Mode: User.


Syntax:
```
show port queue counters {<mod-num> | <mod-swport-range>} [...] [..., {<mod-num> | <mod-swport-range>}]} {ingress | egress | all} [queue <queue>]
```

Table 23-21. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-num&gt;</td>
<td>The slot number of a module. If you specify &lt;mod-num&gt;, the switch displays the QoS statistics for all ports on the module that you specify.</td>
</tr>
</tbody>
</table>
| <mod-swport-range> | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
- To specify port 1 on the module in slot 3, enter 3/1.  
- To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
If you specify <mod-swport-range>, the switch displays the QoS statistics for the port or range of ports that you specify. |
| {ingress | egress | all}             | The direction of traffic that you want to view the QoS Statistics for.  
- Enter ingress to view the QoS statistics for ingress queues.  
- Enter egress to view the QoS statistics for egress queues.  
- Enter all to view the QoS statistics for both ingress and egress queues. |
| <queue>             | The queue number, which can range from 0 to 7. If you do not specify a queue number, the switch displays all QoS statistics for the port or module. |
Sample Output

The following example displays all QoS statistics for the module in slot 3.

```bash
> show port queue counters 3 all
```

Systems

- P550R and P880, 80-series modules only.
- P580 and P882.
show port queue service

**Command Mode**
User.

**Description**
Displays the settings for queue servicing.

**Syntax**
```
show port queue service { <mod-num> | <mod-swport-range> }[,..., { <mod-num> | <mod-swport-range> }]
```

**Sample Output**
The following example displays the queue service settings for port 1 on the module in slot 3

```
> show port queue service 3/1
```

**Systems**
- P550R and P880, 80-series modules only.
- P580 and P882.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-num&gt;</code></td>
<td>The slot number of a module. If you specify <code>&lt;mod-num&gt;</code>, the switch displays queue-service settings for all ports on the module in the slot that you specify.</td>
</tr>
</tbody>
</table>
| `<mod-swport-range>`  | The slot number of a module, and, either a port number, or a range of port numbers having the format Px-Py. For example:  
  - To specify port 1 on the module in slot 3, enter 3/1.  
  - To specify ports 1 through 5 on the module in slot 3, enter 3/1-5.  
  If you specify `<mod-swport-range>`, the switch displays the queue-service settings for the port or range of ports that you specify. |
Overview

This chapter describes the following commands:

- set radius authentication
- set radius authentication group
- set radius authentication realm
- set radius authentication retry-number
- set radius authentication retry-time
- set radius authentication server
- set radius authentication source-ip
- set radius authentication switch-service-type-required
- set radius authentication udp-port
- show radius authentication
set radius authentication

Command Mode  Global Configuration.

Description  Enables or disables RADIUS client.

Syntax

| To Enable: | set radius authentication enabled |
| To Disable: | set radius authentication disabled |

Sample Output  The following command enables RADIUS on the switch:

```
(configure)# set radius authentication enable
```

set radius authentication group

**Command Mode**
Global Configuration.

**Description**
Sets the group to which the switch belongs. If a group is set, then the group name is included in Access Request messages that are sent to the RADIUS server. By default, the switch does not belong to a group.

The group name can be 22 alpha characters.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>set radius authentication group &lt;group&gt;.</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Clear:</td>
<td>clear radius authentication group</td>
</tr>
</tbody>
</table>

**Table 24-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;group&gt;</td>
<td>The group to which the switch belongs. The group name can be 22 characters.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command assigns the switch to group *avaya switches*:

```
(configure)# set radius authentication group avaya switches
```

The following command clears the group membership of the switch:

```
(configure)# clear radius authentication group
```

**Systems**
set radius authentication realm

Command Mode  
Global Configuration.

Description  
Sets the realm of user accounts that are authorized to log in to the switch. Realms are used to organize user accounts.

If a realm is set, @ and the realm name are appended to user login names. For example, the realm name could be Avaya Switches. When user admin logs in, the switch sends the Access Request message for admin@AvayaSwitches. If you set a realm for the switch, you must assign user accounts that are authorized to log in to the switch to the same realm on the RADIUS server.

The realm name can be 22 alpha characters.

Syntax

| To Configure: | set radius authentication realm <realm> |
| To Clear:     | clear radius authentication realm |

Table 24-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;realm&gt;</td>
<td>The realm of user accounts that are authorized to log in to the switch. The realm name can be 22 alpha characters.</td>
</tr>
</tbody>
</table>

Sample Output

The following command sets the realm of authorized user accounts to avaya:

```
(configure) # set radius authentication realm avaya
```

The following command clears the realm of authorized user accounts:

```
(configure) # clear radius authentication realm
```

Systems  
**set radius authentication retry-number**

**Command Mode**  
Global Configuration.

**Description**  
Sets the number of times the switch attempts to contact the RADIUS server to authenticate a user. The default value is 1 retry and the valid range is 0 to 10 retries.

**Syntax**  
set radius authentication retry-number <retry-number>

---

**Table 24-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;retry-number&gt;</td>
<td>The number of times to resend the Access Request message if the RADIUS server does not respond. The default value is 1 retry and the valid range is 0 to 10 retries.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following command sets the number of authentication retries to 4:

```
(configure)# set radius authentication retry-number 4
```

**Systems**  
set radius authentication retry-time

**Command Mode**
Global Configuration.

**Description**
Sets the amount of time in seconds that the switch waits before attempting to reauthenticate a login. The default value is 7 seconds and the valid range is 1 to 30 seconds.

**Syntax**
set radius authentication retry-number `<retry-time-in-seconds>`

**Table 24-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;retry-time-in-seconds&gt;</code></td>
<td>The amount of time in seconds that the switch waits before attempting to reauthenticate a login. The default value is 7 seconds and the valid range is 1 to 30 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command sets the retry time to 10 seconds:

```
(configure) # set radius authentication retry-time 10
```

**Systems**
set radius authentication server

**Command Mode**
Global Configuration.

**Description**
Sets either the primary or secondary RADIUS server settings.

**Syntax**

| To Configure: | set radius authentication server <ip-addr> <shared-secret> [encrypted-type1] [{primary | secondary}] |
|---------------|------------------------------------------------------------------------------------------------------------------|
| To Clear:     | clear radius authentication server [{primary | secondary}] |

**Table 24-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>IP Address of the RADIUS server.</td>
</tr>
<tr>
<td>&lt;shared-secret&gt;</td>
<td>Case sensitive shared secret. This must be exactly the same as on the RADIUS server. Spaces are not allowed.</td>
</tr>
<tr>
<td>[encrypted-type1]</td>
<td>Do not use this option. This option is used by the switch when saving passwords in the startup.txt file.</td>
</tr>
<tr>
<td>[{primary</td>
<td>secondary}]</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command sets the primary RADIUS server to IP address 192.157.1.0 and shared secret to *secret primary*.

```
(configure)# set radius authentication server 192.157.1.0 secret primary
```

**Systems**
set radius authentication source-ip

**Command Mode**
Global Configuration.

**Description**
Sets the IP interface address the switch will use as the source IP address in the Access Request messages. This value must be an IP interface address on the switch. If set, and the IP interface becomes disabled, RADIUS will not function because the switch will not be able to send or receive RADIUS messages.

If left 0.0.0.0 (the default), the switch automatically selects a source IP address from one of its active interfaces. If you use this setting, you must add each of the switch IP addresses to the Client file on the RADIUS server since you are not manually setting the source IP address.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure</th>
<th>set radius authentication source-ip &lt;ip-addr&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Clear</td>
<td>clear radius authentication source-ip</td>
</tr>
</tbody>
</table>

**Table 24-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>IP address that is used as the source IP address for Access Request messages.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command sets the source IP address to 192.168.1.1:

```
(configure)# set radius authentication source-ip 192.168.1.1
```

**Systems**
set radius authentication switch-service-type-required

**Command Mode**  
Global Configuration.

**Description**  
If you enable switch-service-type-required, the switch recognizes only Access Accept messages that have the correct group name included. This setting prevents the switch from incorrectly allowing access to users that may have a user account on the RADIUS server but should not be allowed access to the switch. If this setting is disabled, any user account that is not assigned to a group could log in to the switch.

**Syntax**

| To Enable: | set radius authentication switch-service-type-required enabled |
| To Disable: | set radius authentication switch-service-type-required disabled |

**Sample Output**  
The following command enables the switch-service-type-required setting:

```
(configure)# set radius authentication switch-service-type-required enabled
```

**Systems**  
set radius authentication udp-port

Command Mode
Global Configuration.

Description
Sets the UDP port number used for RADIUS dekagrams. The default is port 1812 with the only options being 1812 or 1645. This must match the UDP port number configured on the RADIUS server.

Syntax
set radius authentication udp-port <1812-or-1645>

Sample Output
The following command sets the udp-port to 1645:

(configure) # set radius authentication udp-port 1645

Systems
show radius authentication

Command Mode User.

Description Displays the current RADIUS configuration. All parameters are displayed with the exception of the shared secrets.

Syntax show radius authentication

Sample Output The following command displays the current RADIUS settings:

```
(configure)# show radius authentication
RADIUS Authentication Configuration
===================================
  Enable State: Disabled
  Primary Server: 10.10.10.6
  Secondary Server: 10.10.10.1
  Source Ip: 10.10.5.6
  Realm:
  Group:
  Retry Number: 1
  Retry Time: 7 seconds
  UDP Port: 1812
  Cajun-Service-Type required: Enabled

Overview

This chapter describes the following commands:

- `snmp-server`
- `snmp-server atm-community`
- `snmp-server community`
- `snmp-server contact`
- `snmp-server engineid`
- `snmp-server group`
- `snmp-server location`
- `snmp-server notify`
- `snmp-server password`
- `snmp-server user`
- `snmp-server view`
- `show snmp`
- `show snmp community`
- `show snmp engineid`
- `show snmp group`
- `show snmp user`
- `show snmp view`
snmp-server

Command Mode
Global Configuration.

Description
Enables or disables the three versions of SNMP: SNMPv1, v2, and v3. This command overrides secure mode, which disables SNMPv1 and v2 and enables SNMPv3. For information on secure mode, see Chapter 4, “Security,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.

Syntax

<table>
<thead>
<tr>
<th>To Enable</th>
<th>snmp-server enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable</td>
<td>no snmp-server</td>
</tr>
</tbody>
</table>

Systems
P580 and P882.
snmp-server atm-community

Command Mode  Global Configuration.

Description  Creates or modifies a community string to access the ATM Uplink module. The no command deletes the community string.

Syntax

| To Configure:            | snmp-server atm-community <community-string> <slot> {ro | rw} [<ip-addr>] |
|--------------------------|--------------------------------------------------------------------------|
| To Delete:               | no snmp-server atm-community <community-string> [<ip-addr>] |

Table 25-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;community-string&gt;</td>
<td>The name of the community string. The community string can range from 1 to 26 characters. Do not assign a community string and SNMPv3 user the same name.</td>
</tr>
<tr>
<td>&lt;slot&gt;</td>
<td>The slot number of the ATM Uplink module.</td>
</tr>
<tr>
<td>ro</td>
<td>Assigns read-only access to the community string.</td>
</tr>
<tr>
<td>rw</td>
<td>Assigns read-write access to the community string.</td>
</tr>
<tr>
<td>[&lt;ip-addr&gt;]</td>
<td>The IP address from which the community string is valid.</td>
</tr>
</tbody>
</table>

Systems  P580 and P882.
**snmp-server community**

**Command Mode**  
Global Configuration.

**Description**  
Creates or modifies a community string to access the switch. The `no` command command deletes the community string.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>snmp-server community <code>&lt;community-string&gt;</code> {group <code>&lt;groupname&gt;</code> [&lt;ip-addr&gt; [notify]]}</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Delete:</td>
<td>no snmp-server community <code>&lt;community-string&gt;</code> [&lt;ip-address&gt;]</td>
</tr>
</tbody>
</table>

**Table 25-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;community-string&gt;</code></td>
<td>The name of the community string. The community string can range from 1 to 26 characters. Do not assign a community string and SNMPv3 user the same name.</td>
</tr>
<tr>
<td><code>&lt;groupname&gt;</code></td>
<td>Name of the group to which you are assigning the community string. <strong>Important</strong>: Do not assign the community string to a group that requires authentication or encryption. Community strings do not support authentication or encryption.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>The IP address from which the community string is valid. Trap messages are sent to this IP address if you enter the <code>notify</code> option.</td>
</tr>
<tr>
<td>[notify]</td>
<td>Sends trap messages to the IP address that you specify.</td>
</tr>
</tbody>
</table>

**Systems**  
P580 and P882.
snmp-server contact

Command Mode  Global Configuration.

Description  Sets the administrative contact for the switch. The switch displays the administrative contact when you enter the show snmp command. The default setting is System Administrator. The no command restores the default setting.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>snmp-server contact &lt;contact-name&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no snmp-server contact</td>
</tr>
</tbody>
</table>

Table 25-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;contact-name&gt;</td>
<td>The name of the administrative contact for the switch.</td>
</tr>
<tr>
<td></td>
<td>The contact name can range from 1 to 127 characters.</td>
</tr>
</tbody>
</table>

Systems  P580 and P882.
**snmp-server engineid**

**Command Mode**  
Global Configuration.

**Description**  
Changes the engine ID of the switch. The default engine ID is based on the IP address of the switch.

After changing the engine ID, you must change all SNMPv3 user passwords. For information on changing SNMPv3 user passwords, see “snmp-server password.”

**Syntax**  
```
snmp-server engineid [ <engine-Id> ]
```

**Table 25-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;engine-Id&gt;</td>
<td>A 12-byte hexadecimal value. Separate each byte with a colon. Example: 00:00:00:09:0a:fe:ff:12:97:33:45:12. <strong>Important:</strong> The last byte of the engine ID must not be greater than EE. If you enter a value greater than EE, you may not be able to access the ATM Uplink module MIBs. The engine ID of an ATM Uplink module is the engine ID of the switch, where the slot number of the ATM Uplink module is added to the last byte. EE is the greatest value that allows for the addition of any one of the 17 slots.</td>
</tr>
</tbody>
</table>

**Systems**  
P580 and P882.
snmp-server group

**Command Mode**
Global Configuration.

**Description**
Creates or modifies a group.

The no command deletes a specific group or all groups of a specific group name (if multiple groups have the same group name). If multiple groups have the same group name, you must enter the appropriate security keyword (noAuth, auth, or priv) to delete one of the groups. If you do not enter a security keyword, all groups of the group name that you enter are deleted.

**CAUTION:**
Avaya recommends that you not modify the predefined groups. When you install v6.0, the existing community strings are assigned to these predefined groups. If you modify them, the community strings may lose their access to the switch. For more information on the migration of existing community strings, Chapter 5, “Configuring SNMP,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.

**Syntax**

| To Configure: | snmp-server group <groupname> {noAuth | auth | priv} [read <readview>] [write <writeview>] [notify <notifyview>] |
|---------------|----------------------------------------------------------------------------------------------------------|
| To Delete:    | no snmp-server group <groupname> {noAuth | auth | priv} |
Table 25-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;readview&gt;</td>
<td>The MIB view to which you want the group to have read access.</td>
</tr>
<tr>
<td>&lt;writeview&gt;</td>
<td>The MIB view to which you want the group to have write access.</td>
</tr>
<tr>
<td>&lt;notifyview&gt;</td>
<td>The MIB view for which you want the group to receive trap messages.</td>
</tr>
</tbody>
</table>

Systems

P580 and P882.
**snmp-server location**

**Command Mode**
Global Configuration.

**Description**
Sets the physical location of the switch. The switch displays the physical location of the switch when you enter the `show snmp` command. The `no` command clears the location.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>snmp-server location <code>&lt;server-location&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Clear:</td>
<td>no snmp-server location</td>
</tr>
</tbody>
</table>

**Table 25-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;server-location&gt;</code></td>
<td>The physical location of the switch. The location can range from 1 to 127 characters.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
snmp-server notify

Command Mode
Global Configuration.

Description
Sets the trap receiver for a community string. The no command clears the trap receiver.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>snmp-server notify &lt;ip-addr&gt; &lt;community-string&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Clear:</td>
<td>no snmp-server notify &lt;ip-addr&gt; &lt;community-string&gt;</td>
</tr>
</tbody>
</table>

Table 25-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address to which you want trap messages sent.</td>
</tr>
<tr>
<td>&lt;community-string&gt;</td>
<td>The existing community string for which you are setting the trap receiver.</td>
</tr>
</tbody>
</table>

Systems
P580 and P882.
snmp-server password

**Command Mode**  Global Configuration.

**Description**  Changes a user password. You must change user passwords when the engine ID changes.

The switch prompts you to enter the new password or passwords. The passwords are case-sensitive and can range from 8 to 64 characters. For security reasons, the CLI does not display the passwords when you enter them.

**Syntax**  

```
snmp-server password <username>
```

**Table 25-8. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;username&gt;</code></td>
<td>The user name for which you want to change the password. The passwords are case-sensitive and can range from 8 to 64 characters.</td>
</tr>
</tbody>
</table>

**Systems**  P580 and P882.
snmp-server user

Command Mode  Global Configuration.

Description  Creates or modifies an SNMPv3 user. The no command deletes an SNMPv3 user.

Syntax

| To Configure: | snmp-server user <username> [group <groupname>] [ [localized] auth {sha | md5} <auth-password> [priv <priv-password>] ] |
| To Delete:    | no snmp-server user <username> |

Table 25-9. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;username&gt;</td>
<td>User name for the SNMPv3 user. The user name can range from 1 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>Important: Do not assign a community string and SNMPv3 user the same name.</td>
</tr>
<tr>
<td>&lt;groupname&gt;</td>
<td>Name of the group to which you are assigning the user.</td>
</tr>
<tr>
<td>localized</td>
<td>Use this keyword if you want to enter the authentication password and privacy password in their localized form instead of text.</td>
</tr>
<tr>
<td></td>
<td>Localized passwords consist of the engine ID plus the password and are then hashed by either HMAC-SHA or HMAC-MD5.</td>
</tr>
<tr>
<td>sha</td>
<td>Authenticates the user by means of HMAC-SHA.</td>
</tr>
<tr>
<td>md5</td>
<td>Authenticates the user by means of HMAC-MD5.</td>
</tr>
</tbody>
</table>


Table 25-9. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
</table>
| `<auth-password>` | The authentication password for the user:  
  - Text passwords can range from 8 to 64 characters.  
  - Localized HMAC-SHA-hashed passwords must be 20 bytes.  
  - Localized HMAC-MD5-hashed passwords must be 16 bytes.  
  Enter all localized passwords in the format of nn:nn:nn:... |
| `<priv-password>` | The encryption password for the user.  
  - Text passwords can range from 8 to 64 characters.  
  - Localized, HMAC-SHA- or HMAC-MD5-hashed encryption passwords must be 16 bytes.  
  Enter all localized passwords in the format of nn:nn:nn:... |

Systems

P580 and P882.
snmp-server view

Command Mode
Global Configuration.

Description
Creates or modifies a MIB view. The no command deletes a view or removes an OID from a view.

Syntax

| To Configure: | snmp-server view <viewname> <OIDST> [{included | excluded}] |
|---------------|-------------------------------------------------------------|
| To Delete:    | no snmp-server view <viewname> [<OIDST>]                     |

Table 25-10. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;viewname&gt;</td>
<td>The name of the view that you want to create or modify. The view name can range from 1 to 32 alphanumeric characters.</td>
</tr>
<tr>
<td>&lt;OIDST&gt;</td>
<td>The object identifier (OID) for the object that you want to either include or exclude from the view. You must enter the numeric OID. Use the wildcard character * to specify a sub-tree family. If used in the no command, the OID is removed from the view.</td>
</tr>
<tr>
<td>{included</td>
<td>excluded}</td>
</tr>
</tbody>
</table>

Systems
P580 and P882.
show snmp

Command Mode  Global Configuration.

Description  Displays the status of SNMP (enabled or disabled) and the administrative contact and physical location of the switch, if set.

Syntax  show snmp

Sample Output  SNMP engine is enabled

Contact Information:  System Administrator

Location Information:  [Location Not Set]

Systems  P580 and P882.
show snmp community

Command Mode  Privileged.

Description  Displays the currently configured community strings.

Syntax  show snmp community [ <community-string> ]

Table 25-11. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;community-string&gt;</td>
<td>The community string for which you want to view the configuration.</td>
</tr>
</tbody>
</table>

Sample Output

<table>
<thead>
<tr>
<th>COMMUNITY</th>
<th>GROUP/ATM</th>
<th>NOTIFY</th>
<th>IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>atm</td>
<td>ATM7</td>
<td>YES</td>
<td>1.2.3.4</td>
</tr>
<tr>
<td>public</td>
<td>normalRO</td>
<td>YES</td>
<td>1.2.3.4</td>
</tr>
</tbody>
</table>

Systems  P580 and P882.
show snmp engineid

**Command Mode**
Global Configuration.

**Description**
Displays the currently configured engine ID of the switch.

**Syntax**
show snmp engineid

**Sample Output**
Engine ID: 00:00:1a:e9:01:0a:14:01:11:00:00:00

**Systems**
P580 and P882.
**show snmp group**

**Command Mode** Privileged.

**Description** Displays the currently configured groups.

**Syntax**
```
show snmp group [<groupname>]
```

**Table 25-12. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;groupname&gt;</code></td>
<td>The group for which you want to view the configuration.</td>
</tr>
</tbody>
</table>

**Sample Output**

<table>
<thead>
<tr>
<th>GROUP</th>
<th>SECURITY</th>
<th>READ</th>
<th>WRITE</th>
<th>NOTIFY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LEVEL</td>
<td>VIEW</td>
<td>VIEW</td>
<td>VIEW</td>
</tr>
<tr>
<td>admin</td>
<td>noAuth</td>
<td>internet</td>
<td>internet</td>
<td>internet</td>
</tr>
<tr>
<td>adminRO</td>
<td>noAuth</td>
<td>admin</td>
<td></td>
<td>admin</td>
</tr>
<tr>
<td>adminRW</td>
<td>noAuth</td>
<td>admin</td>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>initial</td>
<td>noAuth</td>
<td>restricted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>internet</td>
<td>priv</td>
<td>internet</td>
<td>internet</td>
<td>internet</td>
</tr>
<tr>
<td>noAccess</td>
<td>noAuth</td>
<td></td>
<td></td>
<td>internet</td>
</tr>
<tr>
<td>normalRO</td>
<td>noAuth</td>
<td>normal</td>
<td></td>
<td>normal</td>
</tr>
<tr>
<td>normalRW</td>
<td>noAuth</td>
<td>normal</td>
<td>normal</td>
<td>normal</td>
</tr>
</tbody>
</table>

**Systems** P580 and P882.
show snmp user

Command Mode
Privileged.

Description
Displays the currently configured SNMPv3 users.

Syntax
show snmp user [<username>]

Table 25-13. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;username&gt;</td>
<td>The user for which you want to view the configuration.</td>
</tr>
</tbody>
</table>

Sample Output

USER          GROUP     AUTH  PROT  PRIV  
------------------------  ------  -----  ----
admin         admin     NO     NONE  NO   
initial       initial   NO     NONE  NO   
joe           normalRW YES    SHA   NO   

Systems
P580 and P882.
show snmp view

Command Mode  Privileged.

Description  Displays the currently configured views.

Syntax  

show snmp view [viewname]

Table 25-14. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>viewname</td>
<td>The view for which you want to view the configuration.</td>
</tr>
</tbody>
</table>

Sample Output

<table>
<thead>
<tr>
<th>VIEW NAME</th>
<th>TYPE</th>
<th>SUBTREE</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>included</td>
<td>1.3.6.1.*</td>
</tr>
<tr>
<td>admin</td>
<td>excluded</td>
<td>1.3.6.1.6.3.15.*</td>
</tr>
<tr>
<td>admin</td>
<td>excluded</td>
<td>1.3.6.1.6.3.16.*</td>
</tr>
<tr>
<td>normal</td>
<td>included</td>
<td>1.3.6.1.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.6.3.12.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.6.3.13.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.6.3.14.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.6.3.15.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.6.3.16.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.6.3.18.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.4.1.81.37.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.4.1.1751.2.53.*</td>
</tr>
<tr>
<td>normal</td>
<td>excluded</td>
<td>1.3.6.1.4.1.2167.3.1.3.*</td>
</tr>
<tr>
<td>internet</td>
<td>included</td>
<td>1.3.6.1.*</td>
</tr>
<tr>
<td>restricted</td>
<td>included</td>
<td>1.3.6.1.2.1.1.*</td>
</tr>
<tr>
<td>restricted</td>
<td>included</td>
<td>1.3.6.1.2.1.11.*</td>
</tr>
<tr>
<td>restricted</td>
<td>included</td>
<td>1.3.6.1.6.3.10.2.1.*</td>
</tr>
<tr>
<td>restricted</td>
<td>included</td>
<td>1.3.6.1.6.3.11.2.1.*</td>
</tr>
<tr>
<td>restricted</td>
<td>included</td>
<td>1.3.6.1.6.3.15.1.1.*</td>
</tr>
</tbody>
</table>

Systems  P580 and P882.
Overview

This chapter describes the following Secure Shell (SSH) commands:

- clear ssh
- ip ssh
- ssh
- ssh keygen
- ssh timeout
- show ssh
clear ssh

Command Mode  Global Configuration.

Description   Ends an SSH session.

Syntax        clear ssh <session-id>

Table 26-1.  Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Keyword, Argument or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;session-id&gt;</td>
<td>ID of the session that you want to clear. Use the show ssh sessions command to view current SSH sessions and their IDs.</td>
</tr>
</tbody>
</table>

Systems         P580 and P882
**ip ssh**

**Command Mode**
Global Configuration.

**Description**
Enables or disables SSH and changes the port number for SSH.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip ssh {port [&lt;tcp-new-port&gt;] [enable]</th>
<th>[enable]}</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip ssh</td>
<td></td>
</tr>
</tbody>
</table>

**Table 26-2. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Keyword, Argument or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;tcp-new-port&gt;</td>
<td>The port number you want to use for SSH. Valid SSH ports are 22 and 9000 to 65,535. The default port for SSH is port 22.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables SSH.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
**ssh**

**Command Mode**
Global Configuration.

**Description**
Establishes an SSH connection to a remote host.

**Syntax**
```plaintext
ssh [cipher {3des-cbc | blowfish-cbc}] [port <tcp-port>] [user <username>] {<ip-addr> | <hostname>}
```

**Table 26-3. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Keyword, Argument or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des-cbc</td>
<td>Uses 3DES encryption for the SSH session. If you do not specify a cipher, the client can use 3DES or Blowfish. Normally, if the remote host supports 3DES, that is the cipher that is used.</td>
</tr>
<tr>
<td>blowfish-cbc</td>
<td>Uses Blowfish encryption for the SSH session.</td>
</tr>
<tr>
<td>&lt;tcp-port&gt;</td>
<td>The TCP port that you want the client to use for the session. If you do not specify a TCP port, the client uses port 22. Valid ports are 22 and 9000 to 65,535.</td>
</tr>
<tr>
<td>&lt;username&gt;</td>
<td>The user name that you want to use to connect to the remote host. If you do not specify a user name, the user name entering this command is used.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the remote host to which you want to connect.</td>
</tr>
<tr>
<td>&lt;hostname&gt;</td>
<td>The name of the remote host to which you want to connect.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
**ssh keygen**

**Command Mode**
Global Configuration.

**Description**
Generates an SSH server key.

*Important:* If SSH is enabled and you regenerate the SSH server key, you must disable and then reenable SSH for the change to take effect. To disable and reenable SSH, use the `ip ssh` command.

**Syntax**

```
ssh keygen [{rsa | dsa}] [key-size {768 | 1024 | 2048}]
```

**Table 26-4. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Keyword, Argument or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>rsa</td>
<td>Generates an RSA key.</td>
</tr>
<tr>
<td>dsa</td>
<td>Generates a DSA key.</td>
</tr>
<tr>
<td>{768</td>
<td>1024</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
**ssh timeout**

**Command Mode**
Global Configuration.

**Description**
Sets the number of seconds at which an idle connection is disconnected, or restores the default setting of 600 seconds.

**Syntax**

```
ssh timeout [<seconds>]
```

**Table 26-5. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Keyword, Argument or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td>The number of seconds at which you want idle connections disconnected. The valid range is 0 to 1800 seconds. The default setting is 600 seconds. A time out of 0 seconds disables the time out feature. If you do not specify this option, the default setting of 600 seconds is restored.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
show ssh

**Command Mode** User

**Description** Displays the SSH configuration, SSH server key, or current sessions.

**Syntax**

```
show ssh {config | public-key | sessions}
```

**Table 26-6. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Keyword, Argument or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Displays the SSH configuration. The following information is displayed:</td>
</tr>
<tr>
<td></td>
<td>• State of SSH</td>
</tr>
<tr>
<td></td>
<td>• Maximum number of sessions</td>
</tr>
<tr>
<td></td>
<td>• Idle time out. See “ssh timeout.”</td>
</tr>
<tr>
<td></td>
<td>• TCP port</td>
</tr>
<tr>
<td></td>
<td>• Login retry count</td>
</tr>
<tr>
<td></td>
<td>• Available ciphers</td>
</tr>
</tbody>
</table>

**Sample Output** Sample output of the `show ssh sessions` command is as follows:

```
SessionId User     RemoteIp:Port
---------- ------- ------------
0          jsmith  10.10.6.100:1760
1          sjensen 10.10.8.110:1770
2          gschroeder 10.10.7.130:1771
3          tblair  10.10.6.100:1777
```
Sample output of the `show ssh config` command is as follows:

```
SSH Server Configuration
--------------------------
State:   Enabled
Max Sessions:  7
Timeout:  600
TCP Port:  22
Retry Count:  3
Ciphers:   3des-cbc, blowfish-cbc
```

**Systems**

P580 and P882.
Overview

This chapter describes the following Secure Socket Layer (SSL) commands:

- ip https
- show ssl cert
- show ssl certreq
- show ssl ciphers
- show ssl config
- ssl backcert
- ssl certreq
- ssl restart
- ssl selfcert
Chapter 27

**ip https**

**Command Mode**
Global Configuration.

**Description**
Enables or disables SSL/HTTPS.

**Syntax**

| To Enable: | ip https {port [<tcp-new-port>] [enable] | [enable]} |
|------------|------------------------------------------|
| To Disable: | no ip https |

**Table 27-1. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Keyword, Argument or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;tcp-new-port&gt;</td>
<td>The port number you want to use for SSL/HTTPS. Valid ports are 443 or 9000 to 65,535. The default port for SSL/HTTPS is 443.</td>
</tr>
<tr>
<td>enable</td>
<td>Enables SSL/HTTPS.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
show ssl cert

**Command Mode**  
User.

**Description**  
Displays the current SSL server certificate.

**Syntax**  
show ssl cert

**Sample Output**  
Certificate:

```
Data:
  Version: 3 (0x2)
  Serial Number: 1057592590 (0x3f09950e)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=US, ST=Massachusetts, L=Concord, O=Avaya Inc., OU=CCIG, CN=Avaya MultiService Switch/Email=cajunsecurity@avaya.com

  Validity
    Not Before: Jul 7 15:43:10 2003 GMT
    Not After : Jul 6 15:43:10 2013 GMT

  Subject: C=US, ST=Massachusetts, L=Concord, O=Avaya Inc., OU=CCIG, CN=Avaya MultiService Switch/Email=cajunsecurity@avaya.com

  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:aa:69:db:41:17:b0:4f:3c:fb:6c:98:29:ab:c8:
        93:0d:32:c7:ac:60:42:ea:39:02:4e:16:2c:1e:b2:
```
12:8a:ea:19:32:94:d0:d5:1b
Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption

04:9e

**Systems**

P580 and P882.
show ssl certreq

Command Mode
User.

Description
Displays the current certificate signing request (CSR).

Syntax
`show ssl certreq`

Sample Output
Certificate Request:
   Data:
      Version: 0 (0x0)
      Subject: C=us, ST=ma, L=concord, O=avaya, OU=ccig, CN=ccig/Email=techpubs@avaya.com
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
         RSA Public Key: (1024 bit)
         Modulus (1024 bit):
            d4:b1:e8:24:7c:ab:5b:09:c9:29:10:c5:93:08:0e:
         Exponent: 65537 (0x10001)
      Attributes:
         a0:00
         Signature Algorithm: md5WithRSAEncryption
Systems

P580 and P882.
show ssl ciphers

Command Mode
User.

Description
Displays the supported SSL ciphers. The P580 and P882 Multiservice switches support the following cipher suites:

- SSLv3 cipher suites:
  - SSL_RSA_WITH_DES_CBC_SHA
  - SSL_RSA_WITH_3DES_EDE_CBC_SHA

- TLSv1 cipher suites
  - TLS_RSA_WITH_DES_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA

Syntax
show ssl ciphers

Sample Output

    DES-CBC3-SHA SSLv3 Kx=RSA Au=RSA Enc=3DES(168) Mac=SHA1
    DES-CBC-SHA SSLv3 Kx=RSA Au=RSA Enc=DES(56)   Mac=SHA1

Systems
P580 and P882.
show ssl config

Command Mode  User.

Description  Displays the current SSL configuration. The following information is displayed:

- Version of SSL and TLS
- TCP Port
- State of SSL

Syntax  show ssl config

Sample Output

SSL Configuration
-------------------
Version:  SSLv3, TLSv1
TCP Port:  443
State:  Enable

Systems  P580 and P882.
### ssl backcert

**Command Mode**  
Global Configuration.

**Description**  
Reverts to a backup version of the SSL server certificate. If you revert to a backup certificate, the current certificate is renamed and made the backup for later reuse.

**Syntax**  
ssl backcert

**Systems**  
P580 and P882.
ssl certreq

Command Mode
Global Configuration.

Description
Creates a public-private key pair and a certificate signing request (CSR).
You need the following information to create the CSR:

- Two-digit country code
- State or province (full name)
- City
- Organization or company name
- Division or branch name
- Common name (host name of the server)
- E-mail address

After you create the CSR, it is saved to a temporary file in the nonvolatile RAM (NVRAM). Use the “ssl selfcert” command to self sign the CSR.

Syntax
ssl certreq [{512 | 1024}]

Table 27-2. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Keyword, Argument or Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>Creates a public-private key pair of 512 bits.</td>
</tr>
<tr>
<td>1024</td>
<td>Creates a public-private key pair of 1024 bits.</td>
</tr>
</tbody>
</table>

Systems
P580 and P882.
<table>
<thead>
<tr>
<th>ssl restart</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command Mode</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
</tr>
<tr>
<td><strong>Systems</strong></td>
</tr>
</tbody>
</table>
ssl selfcert

Command Mode: Global Configuration.

Description: Self-signs a certificate signing request (CSR).

After self-signing a CSR, you must restart SSL for the certificate to take effect. For information on how to restart SSL, see “ssl restart.”

Syntax: ssl selfcert

Overview

This chapter describes the following commands:

- set port edge admin state
- set port point-to-point admin status
- set port spanning-tree-mode
- set port spantree force-protocol-migration
- set port spantree priority
- set spantree
- set spantree config
- set spantree default-path-cost
- set spantree fwddelay
- set spantree hello
- set spantree hold-count
- set spantree maxage
- set spantree portcost
- set spantree priority
- set spantree version
- show spantree
- show spantree blocked
- show spantree config
- show spantree port
- show spantree version
set port edge admin state

Command Mode Global Configuration.

Description Specifies whether a port is an edge port or a nonedge port. An edge port is not connected to any other bridge. Only edge ports and point-to-point links can rapidly transition to forwarding state.

If you set edge admin state to edge-port, the OperEdgePort field of the show port command is also set to edge-port. However, if the port receives a BPDU, the Oper Edge Port setting changes to non-edge-port. (To receive a BPDU, the port must be connected to a bridge and thus is not an edge port.)

Syntax set port edge admin state <mod-swport-range> [...<mod-swport-range>] {edge-port | non-edge-port}

Table 28-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The module and port or port range.</td>
</tr>
<tr>
<td>edge-port</td>
<td>Defines the port as an edge port.</td>
</tr>
<tr>
<td>non-edge port</td>
<td>Defines the bridge as a nonedge port.</td>
</tr>
</tbody>
</table>

Systems P580 and P882.
set port point-to-point admin status

Command Mode  Global Configuration.

Description  Specifies whether a port is connected to a shared LAN segment or a point-to-point LAN segment. A point-to-point LAN segment is connected to exactly one other bridge (normally with a direct cable between them). Only point-to-point links and edge ports can rapidly transition to forwarding state.

If you set this field to Auto, the switch automatically detects whether the port is connected to a shared link or a point-to-point link. Ports operating in half duplex are set to non-point-to-point, and ports operating in full duplex are set to point-to-point. You can, however, manually set the type of link.

Syntax  set port point-to-point admin status {<mod-num> | <mod-swport-range>} [...,{<mod-num> | <mod-swport-range>}] {force-true | force-false | auto}

Table 28-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The module and port or port range.</td>
</tr>
<tr>
<td>force-true</td>
<td>Defines the port as connected to a point-to-point link.</td>
</tr>
<tr>
<td>force-false</td>
<td>Defines the port as connected to a shared LAN segment.</td>
</tr>
<tr>
<td>auto</td>
<td>Automatically detects whether the port is connected to a shared link or a point-to-point link. Ports operating in half duplex are set to non-point-to-point, and ports operating in full duplex are set to point-to-point. If you select this setting, the OperPointToPoint field of the show port command displays the link type that is detected.</td>
</tr>
</tbody>
</table>

Systems  P580 and P882.
set port spanning-tree-mode

Command Mode  
Global Configuration.

Description  
Enables or disables Spanning Tree on a port.

Syntax

| To Enable: | set port spanning-tree-mode { <mod-num> | <mod-swport-range> } [...{ <mod-num> | <mod-swport-range> }]} enable |
| To Disable: | set port spanning-tree-mode { <mod-num> | <mod-swport-range> } [...{ <mod-num> | <mod-swport-range> }]} disable |

Table 28-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The module and port or port range.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables Spanning Tree on a port. If you disable Spanning Tree on a port, it does not participate in Spanning Tree</td>
</tr>
<tr>
<td>enable</td>
<td>Enables Spanning Tree on a port.</td>
</tr>
</tbody>
</table>

Systems  
set port spantree force-protocol-migration

Command Mode  
Global Configuration.

Description  
Forces a bridge port to send out RSTP BPDUs. By forcing a bridge port to send RSTP BPDUs, you can determine whether legacy 802.1D bridges are present on a LAN segment.

If you remove a legacy 802.1D bridge from a segment, other RSTP bridges on the segment cannot detect the removal so they continue sending STP BPDUs. However, if you force a bridge port to send RSTP BPDUs, they trigger other RSTP bridges on the segment to generate RSTP BPDUs again.

If the switch is running common Spanning Tree, this command has no effect.

Syntax  
set port spantree force-protocol-migration <mod-swport-range> [...<mod-swport-range>] {802.1D | vlan {<vlan-id> | name <vlan-name>}}

Table 28-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The module and port or port range.</td>
</tr>
<tr>
<td>802.1D</td>
<td>Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.</td>
</tr>
</tbody>
</table>
Table 28-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vlan-id&gt;</code></td>
<td>The VLAN ID of the bridge in which the bridge port is participating. Use the <code>vlan &lt;vlan-id&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</td>
</tr>
<tr>
<td><code>&lt;vlan-name&gt;</code></td>
<td>The VLAN name of the bridge in which the bridge port is participating. Use the <code>vlan name &lt;vlan-name&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</td>
</tr>
</tbody>
</table>

Systems

P580 and P882.
set port spantree priority

**Command Mode**
Global Configuration.

**Description**
Sets the priority of a bridge port. A higher priority port (has a lower priority number) is more likely to be chosen as the primary path in the spanning tree when there are two or more paths of equal cost.

The valid range for this field is 0 to 240 in increments of 16. The default setting is 128.

**Syntax**
set port spantree priority <mod-swport-range> [...,<mod-swport-range>] <bport-priority> {802.1D | vlan {<vlan-id> | name <vlan-name>}}

**Table 28-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>The module and port or port range.</td>
</tr>
<tr>
<td>&lt;bport-priority&gt;</td>
<td>Priority of the port as a decimal value. A higher priority port (has a lower priority number) is more likely to be chosen as the primary path in the spanning tree when there are two or more paths of equal cost. The valid range for this field is 0 to 240 in increments of 16. The default setting is 128.</td>
</tr>
<tr>
<td>802.1D</td>
<td>Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.</em></td>
</tr>
</tbody>
</table>
### Table 28-5. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vlan-id&gt;</code></td>
<td>The VLAN ID of the bridge in which the bridge port is participating. Use the <code>vlan </code>&lt;vlan-id&gt;` keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
<tr>
<td><code>&lt;vlan-name&gt;</code></td>
<td>The VLAN name of the bridge in which the bridge port is participating. Use the <code>vlan name </code>&lt;vlan-name&gt;` keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
</tbody>
</table>
**set spantree**

**Command Mode**
Global Configuration.

**Description**
Enable or disable individual spanning tree bridges. The default state is enabled.

**Syntax**

| **To Enable:**                     | set spantree enable {802.1D | vlan {<vlan-id> | name <vlan-name> } } |
|-----------------------------------|--------------------------------------------------------------------------------|
| **To Disable:**                   | set spantree disable {802.1D | vlan {<vlan-id> | name <vlan-name> } } |

**Table 28-6. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables the bridge.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables the bridge.</td>
</tr>
<tr>
<td>802.1D</td>
<td>Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The VLAN ID of the bridge. Use the <code>vlan &lt;vlan-id&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The VLAN name of the bridge. Use the <code>vlan name &lt;vlan-name&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
</tbody>
</table>
Sample Output

The following example disables spanning tree 802.1D protocol on a bridge:

```
(configure) # set spantree disable 802.1D
Bridge successfully disabled
```

Systems

**set spantree config**

**Command Mode**
Global Configuration.

**Description**
Sets the Spanning Tree Protocol configuration. The default setting is per-VLAN.

**Syntax**
set spantree config {ieee | per-vlan | dual-layer | disable}

**Table 28-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ieee</td>
<td>The entire switch is a single IEEE 802.1D-compliant bridge.</td>
</tr>
<tr>
<td>per-vlan</td>
<td>Each VLAN functions as a separate IEEE 802.1D-compliant bridge. VLAN bridges can only be displayed when in per-vlan or dual-layer mode.</td>
</tr>
<tr>
<td>dual-layer</td>
<td>A proprietary version of per-VLAN, where the vlan id is embedded as a tag within the bridge PDUs.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables spanning tree on the switch.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the spanning tree protocol to ieee.

```
(configure)# set spantree config ieee
Config successfully set to ieee
```

**Systems**
set spantree default-path-cost

**Command Mode**
Global Configuration.

**Description**
Sets the type of default path costs that ports in a specific bridge will use. Options are:

- **common-spanning-tree**—uses the 16-bit default path costs from IEEE Std. 802.1D-1998:
  - For 10 MB ports, 100
  - For 100 MB ports, 19
  - For 1 GB ports, 4
  - For 10 GB ports, 3

- **rapid-spanning-tree**—uses the 32-bit default path costs from IEEE Std. 802.1t:
  - 10 Mbps port—2,000,000
  - 100 Mbps port—200,000
  - 1 Gbps port—20,000
  - 10 Gbps port—2,500

*Note:* The switch must be running Rapid Spanning Tree to use the Rapid Spanning Tree default path costs. If the switch is running common Spanning Tree, it uses the common Spanning Tree default path costs regardless of default path cost setting.

**Syntax**
```
set spantree default-path-cost {common-spanning-tree | rapid-spanning-tree} {802.1D | vlan {<vlan-id> | name <vlan-name>}}
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>common-spanning-tree</td>
<td>The 16-bit default path costs from IEEE Std. 802.1D-1998.</td>
</tr>
<tr>
<td>rapid-spanning-tree</td>
<td>The 32-bit default path costs from IEEE Std. 802.1t.</td>
</tr>
<tr>
<td>Name</td>
<td>Definition</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>802.1D</td>
<td>Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
<tr>
<td><code>&lt;vlan-id&gt;</code></td>
<td>The VLAN ID of the bridge. Use the <code>&lt;vlan &lt;vlan-id&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
<tr>
<td><code>&lt;vlan-name&gt;</code></td>
<td>The VLAN name of the bridge. Use the <code>&lt;vlan name &lt;vlan-name&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
</tbody>
</table>

**Rapid Spanning Tree Protocol**

**Systems**

P580 and P882.
set spantree fwddelay

Command Mode
Global Configuration.

Description
Sets the Spanning Tree forward delay time for a bridge. The forward delay time is the time a port takes to change to the forwarding state. The default time is 15 seconds.

Syntax
set spantree fwddelay <fwddelay-value> \{802.1D | vlan {<vlan-id> | name <vlan-name>}}

Table 28-9. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;fwddelay-value&gt;</td>
<td>The forward delay value for the bridge, in seconds. The range is 4-30 seconds. The default setting is 15 seconds.</td>
</tr>
<tr>
<td>802.1D</td>
<td>Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The VLAN ID of the bridge. Use the vlan &lt;vlan-id&gt; keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The VLAN name of the bridge. Use the vlan name &lt;vlan-name&gt; keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</td>
</tr>
</tbody>
</table>
Rapid Spanning Tree Protocol

Sample Output

The following example sets the spanning tree forward delay to 12 seconds.

```
(configure)# set spantree fwddelay 12 802.1D
Bridge Forward Delay Time Successfully set to 12
```

Systems

set spantree hello

**Command Mode**
Global Configuration.

**Description**
Sets the spanning tree bridge hello time. The bridge hello time is the time between generation of BPDUs by the root bridge. The default time is 2 seconds.

**Syntax**
```
set spantree hello <hellotime-value> {802.1D | vlan {<vlan-id> | name <vlan-name>}}
```

**Sample Output**
The following example sets the spanning tree hello time to 5 seconds:
```
(configure)# set spantree hello 5 802.1D
Bridge Hello Time Successfully set to 5
```

**Systems**
set spantree hold-count

**Command Mode**
Global Configuration.

**Description**
Sets the hold count for a bridge.

The *hold count* is the maximum number of BPDUs that are sent out a port in a hello time interval. During any one hello time interval, no more BPDUs than the number that you enter for <hold-count-value> will be sent out a port.

**Syntax**
set spantree hold-count <hold-count-value> {802.1D | vlan {<vlan-id> | name <vlan-name>}}

**Table 28-11. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| <hold-count-value> | The maximum number of BPDUs that are sent out a port in a hello time interval. During any one hello time interval, no more BPDUs than the number that you enter in this field will be sent out a port.  
The valid range for this field is 1 to 10 seconds. The default setting is 3 seconds. |
| 802.1D      | Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1. |
| <vlan-id>   | The VLAN ID of the bridge. Use the vlan <vlan-id> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1 |
| <vlan-name> | The VLAN name of the bridge. Use the vlan name <vlan-name> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1 |

**Systems**
P580 and P882.
set spantree maxage

Command Mode
Global Configuration.

Description
Sets the maximum amount of time that the bridge retains bridging information. When the maximum age expires, the bridge assumes it has lost connection to the network and sends out requests to be readded to the spanning tree. The default age time is 20 seconds.

Syntax
set spantree maxage <maxage-value> {802.1D | vlan {<vlan_id> name <vlan-name>}}

Table 28-12. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;maxage-value&gt;</td>
<td>The maximum amount of time that the bridge retains bridging information. When the maximum age expires, the bridge assumes it has lost connection to the network and sends out requests to be readded to the spanning tree. The valid range for this field is 6 to 40 seconds. The default setting is 20 seconds.</td>
</tr>
<tr>
<td>802.1D</td>
<td>Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The VLAN ID of the bridge. Use the <code>vlan &lt;vlan-id&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The VLAN name of the bridge. Use the <code>vlan name &lt;vlan-name&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</td>
</tr>
</tbody>
</table>
**Sample Output**

The following example sets the spanning tree maximum age to 25 seconds.

```
(configure)# set spantree maxage 25 802.1D
Bridge MaxAge Successfully set to 25
```

**Systems**

set spantree portcost

**Command Mode**  
Global Configuration.

**Description**  
Sets the path cost for this port. The ports that you prefer be used by the spanning tree should have the lowest path cost.

If the switch is running common Spanning Tree, the valid range for this field is 0 to 65535.

If the switch is running Rapid Spanning Tree, the valid range for this field is 0 to 200,000,000.

The default setting is 0. If this field is set to 0, the port uses the default path cost for the bridge.

Common Spanning Tree defaults are:

- 10 Mbps port—100
- 100 Mbps port—19
- 1Gbps port—4
- 10 Gbps port—3

Rapid Spanning Tree defaults are:

- 10 Mbps port—2,000,000
- 100 Mbps port—200,000
- 1 Gbps port—20,000
- 10 Gbps port—2,500
**Syntax**

```
set spantree portcost <mod-swport-range> [...,<mod-swport-range>] ...
<port-cost-value> {802.1D | vlan {<vlan-id> | name <vlan-name>}}
```

---

**Table 28-13. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;mod-swport-range&gt;</code></td>
<td>The module and the port range.</td>
</tr>
</tbody>
</table>
| `<port-cost-value>`         | Sets the path cost for this port. The ports that you prefer be used by the spanning tree should have the lowest path cost.  
If the switch is running common Spanning Tree, the valid range for this field is 0 to 65535.  
If the switch is running Rapid Spanning Tree, the valid range for this field is 0 to 200,000,000.  
The default setting is 0. If this field is set to 0, the port uses the default path cost for the bridge. |
| 802.1D                      | Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1. |
| `<vlan-id>`                  | The VLAN ID of the bridge in which the bridge port is participating.  
Use the `vlan <vlan-id>` keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1 |
| `<vlan-name>`                | The VLAN name of the bridge in which the bridge port is participating.  
Use the `vlan name <vlan-name>` keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1 |
Sample Output  The following example sets the path cost for the bridge.

(configure) # set spantree portcost 5/1 15 802.1D
Port 5/1 path cost successfully set to 15.

set spantree priority

Command Mode  Global Configuration.

Description  Sets the bridge priority for a particular bridge. Enter the priority as hexadecimal value.

The valid range for this field is 0x0000 (0) to 0xF000 (61,440) in increments of 0x1000 (4,096). The default setting is 0x8000 (32,768).

* Note: When you upgrade the switch to v6.0 application software, all bridge priorities are reset to the default setting of 0x8000. Bridge priorities from earlier versions of software are not preserved.

Syntax  set spantree priority <bridge-priority> {802.1D | vlan {<vlan-id> | name <vlan-name>}}

Table 28-14. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;bridge-priority&gt;</td>
<td>The bridge priority, specified as a two byte value in hexadecimal (0x8000). The valid range for this field is 0x0000 (0) to 0xF000 (61,440) in increments of 0x1000 (4,096). The default setting is 0x8000 (32,768).</td>
</tr>
<tr>
<td>802.1D</td>
<td>Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.</td>
</tr>
</tbody>
</table>
### Table 28-14. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vlan-id&gt;</code></td>
<td>The VLAN ID of the bridge. Use the <code>vlan &lt;vlan-id&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
<tr>
<td><code>&lt;vlan-name&gt;</code></td>
<td>The VLAN name of the bridge. Use the <code>vlan name &lt;vlan-name&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in <em>User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</em>.</td>
</tr>
</tbody>
</table>

**Systems**

set spantree version

**Command Mode**  
Global Configuration.

**Description**  
Sets the version of spanning tree that you want the switch to run.

**Syntax**  
set spantree version {common-spanning-tree | rapid-spanning-tree}

### Table 28-15. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>common-spanning-tree</td>
<td>Sets the switch to run Spanning Tree Protocol (STP). When running this mode, the switch generates STP BPDUs.</td>
</tr>
<tr>
<td>rstp</td>
<td>Sets the switch to run Rapid Spanning Tree Protocol (RSTP).</td>
</tr>
</tbody>
</table>

**Systems**  
P580 and P882.
show spantree

Command Mode
User.

Description
Displays information about one or all spanning trees.

Syntax
show spantree {all | 802.1D | vlan {<vlan-id> | name <vlan-name>}}

Table 28-16. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Display all the bridges in configuration mode.</td>
</tr>
<tr>
<td>802.1D</td>
<td>Use this keyword if the switch is running IEEE 802.1D Spanning Tree. For a detailed description of IEEE 802.1D Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The VLAN ID of the bridge.</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The VLAN name of the bridge.</td>
</tr>
</tbody>
</table>

 IEEE mode - Displays only the 802.1D bridge.
 per-vlan or dual-layer mode - Displays all of the VLAN bridges.
**Sample Output**

The following example shows all of the spanning tree bridges that are configured on the switch:

>`show spantree all`

<table>
<thead>
<tr>
<th>Name/Vlan</th>
<th>Status</th>
<th>Bridge ID</th>
<th>Root Port</th>
<th>Root Cost</th>
<th>Designated Root</th>
<th>Top Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>Enabled</td>
<td>0x800100306DBBA000</td>
<td>0x0000</td>
<td>0</td>
<td>0x800100306DBBA000</td>
<td>0</td>
</tr>
<tr>
<td>vlan1</td>
<td>Enabled</td>
<td>0x806500306DBBA000</td>
<td>0x0000</td>
<td>0</td>
<td>0x806500306DBBA000</td>
<td>1</td>
</tr>
<tr>
<td>vlan2</td>
<td>Enabled</td>
<td>0x806600306DBBA000</td>
<td>0x0000</td>
<td>0</td>
<td>0x806600306DBBA000</td>
<td>1</td>
</tr>
<tr>
<td>vlan3</td>
<td>Enabled</td>
<td>0x806700306DBBA000</td>
<td>0x0000</td>
<td>0</td>
<td>0x806700306DBBA000</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name/Vlan</th>
<th>TimeSince TopChange</th>
<th>MaxAge</th>
<th>HelloTime</th>
<th>FwdDelay</th>
<th>Bridge MaxAge</th>
<th>Bridge HelloTime</th>
<th>Bridge FwdDelay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>04:36:40</td>
<td>20</td>
<td>2</td>
<td>15</td>
<td>20</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>vlan1</td>
<td>04:35:44</td>
<td>20</td>
<td>2</td>
<td>15</td>
<td>20</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>vlan2</td>
<td>04:35:44</td>
<td>20</td>
<td>2</td>
<td>15</td>
<td>20</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>vlan3</td>
<td>04:35:44</td>
<td>20</td>
<td>2</td>
<td>15</td>
<td>20</td>
<td>2</td>
<td>15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name/Vlan</th>
<th>Priority</th>
<th>HoldCount</th>
<th>PathCostDefault</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>0x8000</td>
<td>3</td>
<td>rapid-spanning-tree</td>
</tr>
<tr>
<td>vlan1</td>
<td>0x8000</td>
<td>3</td>
<td>rapid-spanning-tree</td>
</tr>
<tr>
<td>vlan2</td>
<td>0x8000</td>
<td>3</td>
<td>rapid-spanning-tree</td>
</tr>
<tr>
<td>vlan3</td>
<td>0x8000</td>
<td>3</td>
<td>rapid-spanning-tree</td>
</tr>
</tbody>
</table>

**Systems**

show spantree blocked

**Command Mode**  
User.

**Description**  
Displays, by VLAN, the ports that are currently in the Blocking state.

**Syntax**  
show spantree blocked

**Sample Output**

<table>
<thead>
<tr>
<th>Mod/Port</th>
<th>PortId</th>
<th>Priority</th>
<th>Number</th>
<th>Role</th>
<th>State</th>
<th>Admin Cost</th>
<th>Oper Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/2</td>
<td>0x80AA</td>
<td>0x80(128)</td>
<td>170</td>
<td>Backup</td>
<td>Discard</td>
<td>0</td>
<td>20000</td>
</tr>
<tr>
<td>6/2</td>
<td>0x80DA</td>
<td>0x80(128)</td>
<td>218</td>
<td>Backup</td>
<td>Discard</td>
<td>0</td>
<td>200000</td>
</tr>
</tbody>
</table>

**Systems**  
P580 and P882.
show spantree config

Command Mode  User.

Description  Displays the current global spanning tree configuration.

Syntax  show spantree config

Sample Output  The following example displays the spanning tree configuration on the switch.

    > show spantree config
    Spanning Tree Config: Per-Vlan

show spantree port

Command Mode
User.

Description
Shows the port attributes for all bridge ports in a particular bridge.

Syntax
show spantree port {802.1D | vlan {<vlan-id> | name <vlan-name>}}

Table 28-17. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1D</td>
<td>Displays all bridge ports in the 802.1D bridge. 802.1D bridges can be viewed only when the switch is running 802.1D Spanning Tree.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The VLAN ID of the bridge for which you want to view bridge ports. Use the <code>vlan &lt;vlan-id&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</td>
</tr>
<tr>
<td>&lt;vlan-name&gt;</td>
<td>The VLAN name of the bridge for which you want to view bridge ports. Use the <code>vlan name &lt;vlan-name&gt;</code> keyword and variable when the switch is running per-VLAN or dual-layer Spanning Tree. For a detailed description of per-VLAN and dual-layer Spanning Tree, see Chapter 7, “Configuring Rapid Spanning Tree,” in User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1</td>
</tr>
</tbody>
</table>
Sample Output

The following example displays the port attributes for the bridge ports on the VLAN configured for 802.1D.

> show spantree port vlan 802.1D

<table>
<thead>
<tr>
<th>Name/Vlan</th>
<th>Status</th>
<th>Bridge ID</th>
<th>Root Port</th>
<th>Root Cost</th>
<th>Designated Root</th>
<th>Top Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan3</td>
<td>Enabled</td>
<td>0x806800306DBBA000</td>
<td>0x0000</td>
<td>0</td>
<td>0x806800306DBBA000</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod/Port</th>
<th>PortId</th>
<th>Priority</th>
<th>Number</th>
<th>Role</th>
<th>State</th>
<th>Admin Cost</th>
<th>Oper Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/4</td>
<td>0x80AC</td>
<td>0x80(128)</td>
<td>172</td>
<td>Desig</td>
<td>Forward</td>
<td>0</td>
<td>19</td>
</tr>
<tr>
<td>7/1</td>
<td>0x8109</td>
<td>0x80(128)</td>
<td>265</td>
<td>Disable</td>
<td>Discard</td>
<td>0</td>
<td>16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod/Port</th>
<th>Designated Root</th>
<th>DesCost</th>
<th>Designated Bridge</th>
<th>DesPort</th>
<th>FwdTrans</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/4</td>
<td>0x806800306DBBA000</td>
<td>0</td>
<td>0x806800306DBBA000</td>
<td>0x80AC</td>
<td>2</td>
</tr>
<tr>
<td>7/1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mod/Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/4</td>
<td>STP</td>
</tr>
<tr>
<td>7/1</td>
<td>-</td>
</tr>
</tbody>
</table>

Systems

show spantree version

Command Mode User.

Description Displays the version of Spanning Tree that the switch is running: either common Spanning Tree or Rapid Spanning Tree Protocol (RSTP).

Syntax show spantree version

Sample Output Spanning Tree Config: Per-Vlan
Protocol Version: common-spanning-tree (0)

Systems P580 and P882.
This chapter describes the following commands:

- set fabric configure-redundant-hardware
- set fabric enable-redundant-element
- set fabric toggle-active-controller
- show fabric status
set fabric configure-redundant-hardware

Command Mode
Global Configuration.

Description
Enables or disables redundant (switch fabric) hardware. The default setting is disabled.

This command does not have reverse mapping. It is not saved to the running or startup configuration file. The configuration is both user and run-time modified.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set fabric configure-redundant-hardware enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set fabric configure-redundant-hardware disable</td>
</tr>
</tbody>
</table>

Sample Output
The following example disables the redundant hardware.

```
(configure) # set fabric configure-redundant-hardware disable
```

Systems
set fabric enable-redundant-element

**Command Mode**
Global Configuration.

**Description**
Sets the enabled redundant element.

This command does not have reverse mapping. It is not saved to the running or startup configuration file. The configuration is both user and run-time modified.

**Syntax**
```
set fabric enable-redundant-element {normal | 1 | 2 | 3 | 4 | 5 | 6}
```

* **Note:** This command is for debug purposes only and is not recommended for use in a production environment.

**Table 29-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{normal</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>• Normal means that the normally enabled redundant element is turned on.</td>
</tr>
<tr>
<td></td>
<td>• 1-6 means that element associated with the number is turned on.</td>
</tr>
</tbody>
</table>

**Systems**
## set fabric toggle-active-controller

**Command Mode**  
Global Configuration.

**Description**  
Toggles the active controller between the current active controller and the (standby) redundant controller.

This command does not have reverse mapping. It is not saved to the running or startup configuration file. The configuration is both user and run-time modified.

**Syntax**  
set fabric toggle-active-controller

*Note: This command is for debug purposes only and is not recommended for use in a production environment.*

**Systems**  
show fabric status

Command Mode User.

Description Displays the switch fabric status.

Syntax show fabric status

Sample Output The following example displays the fabric status.

> show fabric status
Component State
Switch Controller: # 0 Active
Redundant Controller: Available
Switch Elements: Normal # 0
Redundant Element: Available
Enabled Redundant Element Normal

Redundant Hardware Configured

Overview

This chapter describes the following commands:

- boot system flash
- calendar set
- clear utilization high-threshold
- clear utilization monitoring
- clear utilization threshold-event
- clock set
- clock summer-time recurring
- clock timezone
- copy
- copy <filename> running-config
- copy <filename> startup-config
- copy <filename_opt_path> tftp
- copy card-image bootflash
- copy card-image flash
- copy <filename1> pcmcia <filename2>
- copy pcmcia <filename1> <filename2>
- copy running-config
- copy running-config startup-config
- copy running-config tftp
- copy startup-config
- copy startup-config running-config
- copy startup-config tftp
- copy tftp
- copy tftp bootflash
- copy tftp flash
- copy tftp pcmcia
- copy tftp running-config
- copy tftp startup-config
- cpu_redundancy console
- cpu_redundancy hello-interval
- cpu-redundancy mac-prefix
- cpu_redundancy synchronize
- delete pcmcia
- dir
- erase
- erase legacy-configs
- erase scripts
- erase startup-config
- get 48_port_mode
- get Fabric_mode
- hostname
- ip http help server
- nvram initialize
- pcmcia initialize
- reload
- reset
- secure-mode
- set 48_port_mode
- set debug
- set Fabric_mode
- set utilization high-threshold
- set utilization monitoring
- set utilization threshold-event
- setup
- show boot
- show calendar
- show clock
- show cpu
- show cpu_redundancy
- show file_name
- show flash
- show running-config
- show secure-mode
- show snmp
- show startup-config
- show time zone
- show utilization results
- show utilization settings
- show version
### boot system flash

**Command Mode**
Global Configuration.

**Description**
Specifies which system image the switch loads at startup. Configures the image to boot from the FEPROM. The `no` form of this command restores the default system flash setting (app1).

**Syntax**
`boot system flash {app1 | app2 | cardapp1 | cardapp2}`

**Sample Output**
The following example sets the system image that the switch loads at startup to cardapp2 on the pcmcia.

```
(configure)# boot system flash cardapp2
Boot flag set to 'cardapp2'.
```

**Systems**
P580 and P882.

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>app1</td>
<td>app2</td>
</tr>
<tr>
<td>cardapp1</td>
<td>cardapp2</td>
</tr>
</tbody>
</table>
calendar set

Command Mode  Privileged.

Description  Sets the system calendar.

Syntax  
```
calendar set <time> { <date> <month> | <month> <date> } <year>
```

Sample Output  
The following command sets the calendar date.

```
(configure)# calendar set 14:08:00 05 October 1999
```


---

Table 30-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;time&gt;</td>
<td>The time in the format hh:mm:ss.</td>
</tr>
<tr>
<td>&lt;date&gt;</td>
<td>Current day in the month by date.</td>
</tr>
<tr>
<td>&lt;month&gt;</td>
<td>Current month by name.</td>
</tr>
<tr>
<td>&lt;year&gt;</td>
<td>Current year in four digits.</td>
</tr>
</tbody>
</table>
clear utilization high-threshold

Command Mode  Global Configuration.

Description  Resets the high utilization threshold to its default setting of 95 percent. You can reset the high utilization threshold for the CPU, forwarding engines on 80-series media modules, or forwarding engine on the supervisor module.

For the switch to generate events when the high-utilization threshold is exceeded, event logging must be enabled for utilization monitoring. To enable event logging for utilization monitoring, use the set utilization threshold-event command.

Syntax  clear utilization high-threshold {cpu | FIRE | FORE}

Table 30-3. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| cpu  | Resets the high threshold for CPU utilization.  
      100% CPU utilization is the total capacity of the supervisor module to forward slow path traffic. When 100% utilization is reached, the performance of the switch may degrade. |
| FIRE | Resets the high threshold for utilization of the forwarding engines on 80-series media modules.  
      100% FIRE utilization is the total capacity of the forwarding engines on 80-series media modules to forward in band traffic. When 100% utilization is reached, the performance of the switch may degrade. |
| FORE | Resets the high threshold for utilization of the forwarding engine on the supervisor module.  
      100% FORE utilization is the total capacity of the supervisor module to forward out-of-band traffic. When 100% utilization is reached, the performance of the switch may degrade. |

Systems  P580 and P882.
clear utilization monitoring

**Command Mode**
Global Configuration.

**Description**
Disables utilization monitoring for the CPU or forwarding engines. The default setting for utilization monitoring is disabled.

**Syntax**
clear utilization monitoring {cpu | forwarding-engine}

**Table 30-4. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu</td>
<td>Disables monitoring of CPU utilization.</td>
</tr>
<tr>
<td>forwarding-engine</td>
<td>Disables monitoring of 80-series forwarding engines.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
clear utilization threshold-event

Command Mode

Global Configuration.

Description

Disables event logging for utilization monitoring of the CPU or forwarding engines. When event logging is enabled, the switch generates an event if the high-utilization threshold is exceeded.

The default setting for event logging of utilization monitoring is disabled.

Syntax

clear utilization threshold-event {cpu | forwarding-engine}

Table 30-5. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu</td>
<td>Disables event logging for CPU utilization.</td>
</tr>
<tr>
<td>forwarding-engine</td>
<td>Disables event logging for utilization of 80-series forwarding engines.</td>
</tr>
</tbody>
</table>

Systems

P580 and P882.
clock set

Command Mode  Privileged.

Description  Sets the system clock.

Syntax  

\[
\text{clock set } <\text{time}> \{ <\text{date}> <\text{month}> | <\text{month}> <\text{date}> \} <\text{year}>
\]

Sample Output  The following command sets the clock to 2:08 p.m. (14:08:00) on October 5, 2003.

\[
\text{(configure)}\# \text{ clock set 14:08:00 05 October 2003}
\]

Table 30-6. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;time&gt;</td>
<td>The time in the format hh:mm:ss.</td>
</tr>
<tr>
<td>&lt;day&gt;</td>
<td>Current day in the month by name.</td>
</tr>
<tr>
<td>&lt;month&gt;</td>
<td>Current month by name.</td>
</tr>
<tr>
<td>&lt;year&gt;</td>
<td>Current year in four digits.</td>
</tr>
</tbody>
</table>

**clock summer-time recurring**

**Command Mode**
Global Configuration.

**Description**
Configures the switch to automatically change to summer time hours (U.S. Daylight Savings Time). The command format allows for an annual configuration and a one-time change for a particular year. To disable automatic summer time use the `no` form of this command. If parameters are excluded for recurring summer time hours, then summer time is set to default.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>clock summer-time recurring [ &lt;week&gt; &lt;day&gt; &lt;month&gt; <a href="">hh:mm</a> &lt;week&gt; &lt;day&gt; &lt;month&gt; <a href="">hh:mm</a> [ &lt;offset&gt; ] ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] clock summer-time</td>
</tr>
</tbody>
</table>

**Table 30-7. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;week&gt;</td>
<td>Week of the month (1 to 5 (where 5=last)).</td>
</tr>
<tr>
<td>&lt;day&gt;</td>
<td>Day of the week (for example: Sunday, Monday).</td>
</tr>
<tr>
<td>&lt;month&gt;</td>
<td>Month (for example: January, February).</td>
</tr>
<tr>
<td>&lt;date&gt;</td>
<td>Date of the month (1 to 31).</td>
</tr>
<tr>
<td><a href="">hh:mm</a></td>
<td>Time (military format) in hours and minutes.</td>
</tr>
<tr>
<td>&lt;offset&gt;</td>
<td>The number of minutes to add during summer time (default 60). (Optional)</td>
</tr>
</tbody>
</table>

**Sample Output**
The following command sets the recurring summer time hours from the first week of April on Sunday at 2:00 a.m. to the second week in January on Monday at 2:00 a.m.

```
(configure)# clock summer-time recurring 1 Sunday Apr 02:00 2 Mon Jan 02:00
Set of recurring summer time hours succeeded
```

**Systems**
clock timezone

Command Mode        Privileged.

Description        Sets the time zone.

Syntax             clock timezone {<zone-name> | <hours> [<minutes>]}
**copy**

**Command Mode** Privileged.

**Description** Copy a specified file in NVRAM to another specified file in NVRAM.

**Syntax**

```
copy <source filename> <dest filename>
```

**Table 30-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;source filename&gt;</code></td>
<td>The name of the source file in NVRAM. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;</td>
</tr>
<tr>
<td><code>&lt;dest filename&gt;</code></td>
<td>The name of the destination file in NVRAM. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example shows the `copy <source filename> <dest filename>` command.

```
# copy ripcfg.txt test.txt
Copied file '/NVRAM/ripcfg.txt' to file '/NVRAM/test.txt'
```

copy <filename> running-config

Command Mode  
Global Configuration.

Description  
Executes the specified file in NVRAM. The running (current) configuration displays as a merge of the executed file and the existing configuration, with the executed file taking precedence.

Syntax  
copy <filename> running-config

Table 30-10. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename&gt;</td>
<td>The name of the file in NVRAM. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of ”.txt”</td>
</tr>
</tbody>
</table>

Sample Output  
The following example shows the copy <filename> running-config command.

```
(configure)# copy 51.txt running-config
Executing script ’/NVRAM/51.txt’...
Script output written to file ’logfile.txt’.
```

Systems  
copy `<filename>` startup-config

**Command Mode**  
Privileged.

**Description**  
Copies the specified file located in NVRAM to the startup (bootup) configuration.

**Syntax**  
`copy `<filename>` startup-config`

**Table 30-11. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The name of the file in NVRAM. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;txt&quot;</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example shows the copy `<filename>` startup-config command.

```
# copy ripcfg.txt startup-config
Copied file '/NVRAM/ripcfg.txt' to file '/NVRAM/startup.txt'
```

**Systems**  
copy <filename_opt_path> tftp

Command Mode
Privileged.

Description
Uploads a specified file in NVRAM to a specified TFTP server.

Syntax
copy <filename_opt_path> tftp <ip-addr>

Table 30-12. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename_opt_path&gt;</td>
<td>The name of the file in NVRAM. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the TFTP server</td>
</tr>
</tbody>
</table>

Sample Output
The following example shows the copy <filename_opt_path> tftp <ip-addr> command.

# copy jadams/test.txt tftp 205.181.0.205
Copied file 'test.txt' to file 'jadams/test.txt' on TFTP server 205.181.0.205

Systems
copy card-image bootflash

**Command Mode**  
Privileged.

**Description**  
Copies card FLASH images to and from the PCMCIA flash card.

**Syntax**  
copy card-image bootflash {boot | cardboot} {boot | cardboot}

**Sample Output**  
The following example copies the boot image from boot to cardboot.

```
# copy card-image bootflash boot cardboot
```

**Systems**  
P580 and P882.

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{boot</td>
<td>cardboot}</td>
</tr>
</tbody>
</table>
**copy card-image flash**

**Command Mode**  
Global Configuration.

**Description**  
Copies card FLASH images to and from the PCMCIA flash card.

**Syntax**  
copy card-image flash {app1 | app2 | cardapp1 | cardapp2} {app1 | app2 | cardapp1 | cardapp2}

**Table 30-14. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{app1</td>
<td>app2</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example copies the flash image from app1 to cardapp2.

```
(configure)# copy card-image flash app1 cardapp2
Copied file ‘jadams/test.txt’ from TFTP server 205.181.0.205 to ’test.txt’
```

**Systems**  
P580 and P882.
**copy <filename1> pcmcia <filename2>**

**Command Mode**
Global Configuration.

**Description**
Copies a file `<filename1>` from the /NVRAM file system to the /pcmcia file system `<filename2>`.

**Syntax**
copy `<filename1>` pcmcia `<filename2>`

**Table 30-15. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename1&gt;</code></td>
<td>File from /NVRAM files system.</td>
</tr>
<tr>
<td><code>&lt;filename2&gt;</code></td>
<td>File to /pcmcia file system.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example copies a file from NVRAM to PCMCIA.

```plaintext
(configure)# copy boston.txt pcmcia boston2.txt
Copied file 'boston.txt' from /NVRAM system to /pcmcia system.
```

**Systems**
P580 and P882.
**copy pcmcia <filename1> <filename2>**

**Command Mode**
Global Configuration.

**Description**
Copies a file `<filename1>` from the `/pcmcia` file system to the NVRAM file system `<filename2>`.

**Syntax**
copy pcmcia `<filename1>` `<filename2>`

### Table 30-16. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename1&gt;</code></td>
<td>File from <code>/pcmcia</code> files system.</td>
</tr>
<tr>
<td><code>&lt;filename2&gt;</code></td>
<td>File to <code>/NVRAM</code> file system.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example copies a file from PCMCIA to NVRAM.

```
(configure)# copy pcmcia jerry.txt jerry2.txt
Copied file 'jerry.txt' from /pcmcia system to /NVRAM system.
```

**Systems**
P580 and P882.
**copy running-config**

**Command Mode**
Privileged.

**Description**
Saves the running configuration to a file in NVRAM.

**Syntax**
copy running-config <filename>

**Table 30-17. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename&gt;</td>
<td>The name of the destination file in NVRAM. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example shows the copy running-config command.

```
# copy running-config text.txt
Wrote running-config to ’/NVRAM/test.txt’
```

**Systems**
copy running-config startup-config

**Command Mode** Privileged.

**Description** Saves the running (current) configuration as the startup (bootup) configuration in NVRAM.

**Syntax**

```
copy running-config startup-config
```

**Sample Output**

The following example shows the copy running-config startup-config command.

```
# copy running-config startup-config
Wrote running-config to '/NVRAM/startup.txt'
```

copy running-config tftp

Command Mode  Privileged.

Description  Uploads the running (current) configuration to the specified filename on the specified TFTP server.

Syntax  
```
copy running-config tftp <filename_opt_path> <ip-addr>
```

Table 30-18. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename_opt_path&gt;</code></td>
<td>The filename with optional path, which may include a relative sub-directory name. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>The IP address of the TFTP server</td>
</tr>
</tbody>
</table>

Sample Output  The following example shows the copy running-config tftp command.

```
# copy running-config tftp jadams/running.txt 205.181.0.205
Copied running-config to file ‘jadams/running.txt’ on TFTP server 205.181.0.205
```

copy startup-config

Command Mode
Privileged.

Description
Copy the startup (bootup) configuration to the specified file in NVRAM.

Syntax
copy startup-config <filename>

Table 30-19. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename&gt;</td>
<td>The name of the destination file in NVRAM. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;.</td>
</tr>
</tbody>
</table>

Sample Output
The following example shows the copy startup-config command.

# copy startup-config text.txt
Copied file '/NVRAM/startup.txt' to file '/NVRAM/test.txt'

Systems
copy startup-config running-config

Command Mode  Global Configuration.

Description  Executes the startup (bootup) configuration. The running (current) configuration displays as a merge of the executed file and the existing configuration, with the executed file taking precedence.

Syntax  
copy startup-config running-config

Systems  The following example shows the copy startup-config running-config command.

  (configure)# copy startup-config running-config
  Executing script '/NVRAM/startup.txt'...
  Script output written to file 'logfile.txt'.

**copy startup-config tftp**

**Command Mode**  
Privileged.

**Description**  
Uploads the startup (bootup) configuration to the specified file on the specified TFTP server.

**Syntax**  
copy startup-config tftp <filename_opt_path> <ip-addr>

---

**Table 30-20. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename_opt_path&gt;</td>
<td>The name of the destination file in NVRAM. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the TFTP server.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example shows the copy startup-config tftp command.

```
#  copy startup-config tftp jadams/startup.txt 205.181.0.205
Copied startup-config to file 'jadams/startup.txt' on TFTP server 205.181.0.205
```

**Systems**  
**copy tftp**

**Command Mode** Privileged.

**Description** Copies the specified file from the specified TFTP server to NVRAM.

**Syntax**

```
copy tftp <filename_opt_path> <ip-addr>
```

**Sample Output**

The following example copies a file from a TFTP server to NVRAM.

```
# copy tftp jadams/test.txt 205.181.0.205
Copied file 'jadams/test.txt' from TFTP server 205.181.0.205 to 'test.txt'
```

**Systems**


---

**Table 30-21. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename_opt_path&gt;</td>
<td>The name of the file on the TFTP server and in NVRAM, which may include a relative sub-directory name on the TFTP server. It must have a 1-8 letter base filename, and a three letter file extension.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the TFTP server.</td>
</tr>
</tbody>
</table>
copy tftp bootflash

Command Mode  Global Configuration.

Description  Copies a specified binary boot image from a specified TFTP server to bootflash.

Syntax  
\[
\text{copy tftp bootflash } <\text{image_opt_path}> <\text{tftp-server}>
\]

Table 30-22. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;image_opt_path&gt;</td>
<td>The name of the binary image on the TFTP server; which may include a relative</td>
</tr>
<tr>
<td></td>
<td>sub-directory name.</td>
</tr>
<tr>
<td>&lt;tftp-server&gt;</td>
<td>The IP address of the TFTP server.</td>
</tr>
</tbody>
</table>

Sample Output  The following example copies a boot image from a TFTP server to bootflash.

\[
\text{(configure)\# } \text{copy tftp bootflash m55rboot_v3.0.0.bin} 205.181.0.205
\]

Received good file header.
Memory erase in progress.
Memory erase successfully completed.
Transfer in progress ...
Transferred 125952 bytes of m55rboot_v3.0.0.bin
Transferred 197120 bytes of m55rboot_v3.0.0.bin
Transferred 266240 bytes of m55rboot_v3.0.0.bin
Transferred 334848 bytes of m55rboot_v3.0.0.bin
Transferred 403456 bytes of m55rboot_v3.0.0.bin
Transferred 467456 bytes of m55rboot_v3.0.0.bin
Transferred 521096 bytes of m55rboot_v3.0.0.bin
Copied file ‘m55rboot_v3.0.0.bin’ from TFTP server 205.181.0.205 to BOOT

**copy tftp flash**

**Command Mode**  
Global Configuration.

**Description**  
Copies a specified binary image from a specified TFTP server to the flash location APP1 or APP2.

**Syntax**  
```
copy tftp flash {app1 | app2} <image_opt_path> <ip-addr>
```

**Sample Output**  
The following example copies a boot image from a TFTP server to bootflash.

```
(configure)# copy tftp flash app1 m5500r_a4.0.2.bin 205.181.0.205
Received good file header.
Memory erase in progress.
Memory erase successfully completed.
Transfer in progress ...
    Transferred 143872 bytes of m5500r_a4.0.2.bin
    Transferred 219136 bytes of m5500r_a4.0.2.bin
    Transferred 295936 bytes of m5500r_a4.0.2.bin
    Transferred 372736 bytes of m5500r_a4.0.2.bin
    Transferred 449536 bytes of m5500r_a4.0.2.bin
```

Copied file ‘m5500r_a4.0.2.bin’ from TFTP server 205.181.0.205 to APP1

**Systems**  

---

**Table 30-23. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{app1</td>
<td>app2}</td>
</tr>
<tr>
<td>&lt;image_opt_path&gt;</td>
<td>The name of the binary image on the TFTP server; which may include a relative sub-directory name.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the TFTP server.</td>
</tr>
</tbody>
</table>
**copy tftp pcmcia**

**Command Mode**  
Global Configuration.

**Description**  
Copies a specified binary image from a specified TFTP server to the PCMCIA flash card.

**Syntax**  
`copy tftp pcmcia {cardapp1 | cardapp2} <image_opt_path> <ip-addr>`

**Table 30-24. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{cardapp1</td>
<td>cardapp2}</td>
</tr>
<tr>
<td>&lt;image_opt_path&gt;</td>
<td>The name of the binary image on the TFTP server. This field name may include a relative sub-directory name.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the TFTP server.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example copies a boot image from a TFTP server to cardapp2 on the PCMCIA card:

```plaintext
(configure)# copy tftp pcmcia cardapp2 m5500r_a4.0.2.bin 205.181.0.205
Received good file header.
Memory erase in progress.
Memory erase successfully completed.
Transfer in progress ...  
Transferred 143872 bytes of m5500r_a5.0.12.bin
Transferred 219136 bytes of m5500r_a5.0.12.bin
Transferred 295936 bytes of m5500r_a5.0.12.bin
Transferred 372736 bytes of .
```

**Systems**  
P580 and P882.
copy tftp running-config

**Command Mode**  
Global Configuration.

**Description**  
Copies a specified filename from a specified TFTP server, and executes a script. The running configuration displays as merge of the executed file and the existing configuration, with the executed file taking precedence.

**Syntax**  
copy tftp running-config `<filename_opt_path>` `<ip-addr>`

**Table 30-25. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename_opt_path&gt;</code></td>
<td>The name of the file on the TFTP server; may include a relative sub-directory name. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;.</td>
</tr>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>The IP address of the TFTP server.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example copies the indicated file to the running-config file.

```
(configure)# copy tftp running-config jadams/ripcfg.txt
205.181.0.205
Executing script '/NVRAM/ripcfg.txt'...
Script output written to file 'logfile.txt'.
Copied file 'jadams/ripcfg.txt' from TFTP server 205.181.0.205 to running-config
```

**Systems**  
copy tftp startup-config

Command Mode  Privileged.

Description Copies a specified file from a specified TFTP server to the startup (bootup) configuration in NVRAM.

Syntax copy tftp startup-config <filename_opt_path> <ip-addr>

Table 30-26. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename_opt_path&gt;</td>
<td>The name of the file on the TFTP server; may include a relative sub-directory name. It must be an ASCII script file, with a 1-8 letter base filename, and file extension of &quot;.txt&quot;.</td>
</tr>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The IP address of the TFTP server.</td>
</tr>
</tbody>
</table>

Sample Output The following example copies the indicated file to the startup configuration file.

```
# copy tftp startup-config jadams.txt 205.181.0.205
Copied file ‘jadams.txt’ from TFTP server 205.181.0.205 to startup-config
```

cpu_redundancy console

**Command Mode**
Global Configuration.

**Description**
Changes the ethernet console IP address for the supervisor module in the specified slot.

**Syntax**
```
cpu_redundancy console {slot1 | slot2} <ip-addr>
```

**Table 30-27. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-addr&gt;</td>
<td>The new IP address of the Ethernet console.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example changes the ethernet console IP address of the supervisor module in slot 2.

```
(configure) # cpu_redundancy console slot2 1.1.1.1
```

**Systems**
cpu_redundancy hello-interval

**Command Mode**

Global Configuration.

**Description**

Sets the hello time in seconds for the standby supervisor. The valid range is 1 to 300 seconds. The default setting is 5 seconds. The **no** command restores the default setting.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>cpu_redundancy hello-interval <code>&lt;seconds&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no cpu_redundancy hello-interval</td>
</tr>
</tbody>
</table>

**Table 30-28. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;seconds&gt;</code></td>
<td>Hello-time in seconds. The valid range is 1 to 300 seconds. The default setting is 5 seconds.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example sets the hello time for the standby supervisor to 2 seconds.

```
(configure)# cpu_redundancy hello-interval 2
```

**Systems**

cpu-redundancy mac-prefix

**Command Mode**
Global Configuration.

**Description**
Resets the MAC prefix for the standby supervisor.

**Syntax**
cpu_redundancy mac-prefix reset

**Systems**
cpu_redundancy synchronize

Command Mode  Global Configuration.

Description  Synchronizes the active and standby supervisor modules.

Syntax  cpu_redundancy synchronize

Sample Output  The following example synchronizes the active and standby supervisor modules.

   (configure)# cpu_redundancy synchronize

delete pcmcia

Command Mode         Global Configuration.

Description          Deletes a file from the /pcmcia flash card file system.

Syntax               delete pcmcia <filename>

Sample Output        The following example deletes the jerry2.txt from to /pcmcia card file system.

                        (configure) # delete pcmcia jerry2.txt
                        Jerry2.txt deleted

Table 30-29. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename&gt;</td>
<td>File to delete from the /pcmcia card file system.</td>
</tr>
</tbody>
</table>

Systems             P580 and P882.
dir

**Command Mode**  
User.

**Description**  
Displays a directory listing of a single file or all files located in NVRAM.

**Syntax**  
`dir [<filename>]`

---

### Table 30-30. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The name of the file in NVRAM. It must have a 1-8 letter base filename, and a 3 letter file extension. No wildcards are permitted.</td>
</tr>
</tbody>
</table>

---

**Sample Output**  
The following example displays all of the files currently in NVRAM.

```
> dir
Device Name       Capacity (Bytes) Available (Bytes) Utilization
NV Device        523968          480064         9%

-#- -Length- ---Date/Time--- ----Name----
1   5        03-Aug-28 04:06  panic.int
2   35457    03-Oct-23 14:50  shutdown.log
3   13       03-Sep-30 15:23  console.int
4   76       03-Sep-30 15:23  modem.int
5   3        03-Sep-30 15:24  swfabric.int
6   1        03-Aug-28 11:06  buffer.int
7   36       03-Sep-30 15:24  aftPle.int
8   505      03-Sep-30 15:24  rmonsmpl.int
9   1214     03-Oct-07 15:50  startup.txt
11  25       03-Aug-28 11:07  loopbk.int
13  1025     03-Aug-28 11:06  server.crt
15  2142     03-Sep-30 15:24  logfile.txt
```

**Systems**  
erase

**Command Mode**  Privileged.

**Description**  Erases the specified file from NVRAM.

**Syntax**  

```
erase <filename>
```

---

**Table 30-31. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;filename&gt;</code></td>
<td>The name of the file in NVRAM. It must have a 1-8 letter base filename, and a three letter file extension. No wildcards are permitted.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example erases the test.txt file from NVRAM.

```
# erase test.txt
File '/NVRAM/test.txt' deleted.
```

**Systems**  
erase legacy-configs

**Command Mode**
Privileged.

**Description**
Erases all legacy (v3.x and earlier) configurations (.cfg files) from NVRAM. If you do not plan on going back to 3.x code, this command makes it possible for you to free NVRAM space on your system easily.

**Syntax**
erase legacy-configs

**Sample Output**
The following example erases all legacy configurations from NVRAM.

```
# erase legacy-configs
Successfully deleted all Configuration files from the system.
```

**Systems**
**erase scripts**

**Command Mode**  
Privileged.

**Description**  
Erases all ASCII script files (.txt files) from NVRAM. This command is useful for cleaning up NVRAM, but you should copy the startup configuration to a TFTP server first, or copy the running configuration to the startup configuration afterward.

**Syntax**  
`erase scripts`

**Sample Output**  
The following example erases all ASCII script files from NVRAM.

```
# erase scripts
Successfully deleted all Text files from the system.
```

**Systems**  
### erase startup-config

**Command Mode**  
Privileged.

**Description**  
Erases the startup (bootup) configuration from NVRAM.

**Syntax**  
erase startup-config

**Sample Output**  
The following example erases the startup configuration from NVRAM.

```
# erase startup-config
File '/nvram/startup.txt' deleted.
```

**Systems**  
get 48_port_mode

Command Mode  Global Configuration.

Description  Displays the status of 48-port mode.

If you install an 80-series, 48-port, 10/100 module with Telco connectors (M8048R-100TC) in a switch, you must enable 48-port mode for the module to operate.

Syntax  get 48_port_mode

Sample Output  The following example displays the status of 48-port mode:

(configure)# get 48_port_mode
Current Configuration is 48-Port Modules Enabled

### get Fabric_mode

**Command Mode**
Global Configuration.

**Description**
Displays the Fabric mode that the switch is currently operating in.

To change the Fabric mode setting and speed that the switch operates at, use the `set Fabric_mode` command. For information on the `set Fabric_mode` command, see “set Fabric_mode.”

**Syntax**
```
get Fabric_mode
```

**Sample Output**
The following example displays the Fabric mode that the switch is operating in:

```
(configure)# get Fabric_mode
Current Configuration is Fabric Mode 1
Current system speed is 55 MHz
```

**Systems**
hostname

**Command Mode**  
Global Configuration.

**Description**  
Specifies the hostname that is displayed in the system prompts and default configuration filenames. Use the **no** form of the command to disable the hostname currently being used.

**Syntax**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Enable:</strong></td>
<td>hostname <code>&lt;host-name&gt;</code></td>
</tr>
<tr>
<td><strong>To Disable:</strong></td>
<td><code>[no] hostname</code></td>
</tr>
</tbody>
</table>

**Table 30-32. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;host-name&gt;</code></td>
<td>Name of the host.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following command configures the hostname as *Avaya 23*.

```
(configure)# hostname Avaya 23
Avaya 23(configure)#
```

**Systems**  
ip http help server

Command Mode
Global Configuration.

Description
Configures the HTTP server for online help. The no form of this command clears the server location.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip http help server &lt;url&gt; &lt;directory&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip http help server</td>
</tr>
</tbody>
</table>

Table 30-33. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;url&gt;</td>
<td>The universal resource locator (URL) for the help server.</td>
</tr>
<tr>
<td>&lt;directory&gt;</td>
<td>The name of the directory containing the help files.</td>
</tr>
</tbody>
</table>

Sample Output
The following example configures the HTTP server for online help.

(configure)# ip http help server 1.1.1 help

Systems
nvram initialize

Command Mode       Global Configuration.

Description        Resets all switch settings except the following to their default values:
                     ■ Startup image
                     ■ Fabric mode
                     ■ 48-port mode

Syntax              nvram initialize

Sample Output       The following example initializes NVRAM.
                     
                     (configure)# nvram initialize
                     This command will restore all configuration settings to factory defaults.
                     Are you sure you want to continue? (Y/N)
                     NV is initialized ... reboot to take effect.

## pcmcia initialize

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Initializes the PCMCIA card.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td>pcmcia initialize</td>
</tr>
<tr>
<td><strong>Sample Output</strong></td>
<td>The following example initializes the PCMCIA card installed in the PCMCIA carrier on the Supervisor module.</td>
</tr>
<tr>
<td></td>
<td>(configure)# <strong>pcmcia initialize</strong></td>
</tr>
<tr>
<td><strong>Systems</strong></td>
<td>P580 and P882.</td>
</tr>
</tbody>
</table>
reload

Command Mode  Global Configuration.

Description  Reloads the switch software.

Syntax  reload

Sample Output  The following example reloads the switch software.

    (configure)# reload
    Booting the operational system, please wait ....

    Initializing the event subsystem ... done
    Initializing the agent subsystem ... initializing
    AppleTalk...done
    done
    Initializing the platform ...
      Resetting Thunderbolt ...done.
    Setting module to MASTER and resetting chips
    ...done.
    Creating Ethernet Console ...done.
    Creating Display Manager ...done.
    done
    .
    .
    .

reset

Command Mode  Global Configuration.

Description  Resets the switch and reloads the software.

Syntax  reset

Sample Output  The following example resets the switch and reloads the software.

        (configure)# reset

secure-mode

**Command Mode**  
Global Configuration.

**Description**  
Enables and disables secure mode. Secure mode restricts management of the switch to the following secure protocols:

- HTTPS
- SSH
- SNMPv3

When you enable secure mode, all non-secure protocols, such as Telnet, HTTP, and SNMPv1 and v2 are automatically disabled.


**Syntax**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Enable:</strong></td>
<td>secure-mode</td>
</tr>
<tr>
<td><strong>To Disable:</strong></td>
<td>no secure-mode</td>
</tr>
</tbody>
</table>

**Systems**  
P580 and P882.
set 48_port_mode

Command Mode Global Configuration.

Description Enables 48-port mode on the switch.

If you install an 80-series, 48-port, 10/100 module with Telco connectors (M8048R-100TC) in a switch, you must enable 48-port mode for the module to operate.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set 48_port_mode enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set 48_port_mode disable</td>
</tr>
</tbody>
</table>

set debug

Command Mode  Global Configuration.

Description  Enables debug mode for troubleshooting. The default is off.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>set debug on</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>set debug off</td>
</tr>
</tbody>
</table>

Sample Output  The following example enables debug command.

(configure) # set debug on

set Fabric_mode

**Command Mode**  
Global Configuration.

**Description**  
Sets the Fabric mode setting and speed that the switch operates at. Fabric mode 1 operates at 55 MHz. Fabric mode 2 operates at 66 MHz.

Only P580 and P882 chassis that contain all 80-series modules support Fabric mode 2.

To view the current Fabric mode setting, use the `get Fabric_mode` command. For information on the `get Fabric_mode` command, see "get Fabric_mode."

**Syntax**  
set Fabric_mode {1 | 2}

**Table 30-34. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| {1 | 2}  | • Enter 1 to set the switch to Fabric mode 1 and 55 MHz.  
|       | OR                                                                         |
|       | • Enter 2 to set the switch to Fabric mode 2 and 66 MHz.                   |

**Systems**  
set utilization high-threshold

Command Mode

Global Configuration.

Description

Sets the high utilization threshold at which the switch generates an event. You can set a high utilization threshold for the CPU, forwarding engines on 80-series media modules, or forwarding engine on the supervisor module. The default setting for the utilization threshold is 95 percent. Clearing the utilization threshold resets it to 95 percent, its default setting.

For the switch to generate events when the high-utilization threshold is exceeded, event logging must be enabled for utilization monitoring. To enable event logging for utilization monitoring, use the set utilization threshold-event command.

Syntax

| To Configure: | set utilization high-threshold {cpu | FIRE | FORE} <utilization-percent> |
|---------------|---------------------------------------------------------------------|
| To Restore Default: | clear utilization high-threshold {cpu | FIRE | FORE} |

Table 30-35. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu</td>
<td>Sets the high threshold for CPU utilization. 100% CPU utilization is the total capacity of the supervisor module to forward slow path traffic. When 100% utilization is reached, the performance of the switch may degrade.</td>
</tr>
<tr>
<td>FIRE</td>
<td>Sets the high threshold for utilization of the forwarding engines on 80-series media modules. 100% FIRE utilization is the total capacity of the forwarding engines on 80-series media modules to forward in band traffic. When 100% utilization is reached, the performance of the switch may degrade.</td>
</tr>
</tbody>
</table>
**System**

P580 and P882.

---

**Table 30-35. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>FORE</td>
<td>Sets the high threshold for utilization of the forwarding engine on the supervisor module. 100% FORE utilization is the total capacity of the supervisor module to forward out-of-band traffic. When 100% utilization is reached, the performance of the switch may degrade.</td>
</tr>
<tr>
<td><code>&lt;utilization-percent&gt;</code></td>
<td>The high threshold at which you want the switch to log an event in the event log. Enter a value from 50 through 99. The default setting is 95.</td>
</tr>
</tbody>
</table>

2 of 2
**set utilization monitoring**

**Command Mode**  
Global Configuration.

**Description**  
Enables utilization monitoring for the CPU or forwarding engines. The default setting for utilization monitoring is disabled.

**Syntax**

| To Enable:                        | set utilization monitoring {cpu | forwarding-engine} |
|-----------------------------------|-----------------------------------------------------|
| To Disable:                       | clear utilization monitoring {cpu | forwarding-engine} |

**Table 30-36. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu</td>
<td>Enables monitoring of CPU utilization.</td>
</tr>
<tr>
<td>forwarding-engine</td>
<td>Enables monitoring of 80-series forwarding engines.</td>
</tr>
</tbody>
</table>

**Systems**  
P580 and P882.
set utilization threshold-event

**Command Mode**
Global Configuration.

**Description**
Enables event logging for utilization monitoring of the CPU or forwarding engines. When event logging is enabled, the switch generates an event if the high-utilization threshold is exceeded.

The default setting for event logging of utilization monitoring is disabled. If you enable event logging for utilization monitoring but do not specify a utilization threshold, the switch logs an event if the CPU utilization or forwarding engine utilization exceeds 95 percent. To change the utilization threshold, use the `set utilization high-threshold` command.

**Syntax**

| To Enable:               | set utilization threshold-event {cpu | forwarding-engine} |
|--------------------------|------------------------------------------------------------|
| To Disable:              | clear utilization threshold-event {cpu | forwarding-engine} |

**Table 30-37. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu</td>
<td>Enables event logging for CPU utilization.</td>
</tr>
<tr>
<td>forwarding-engine</td>
<td>Enables event logging for utilization of 80-series forwarding engines.</td>
</tr>
</tbody>
</table>

**Systems**
P580 and P882.
**setup**

**Command Mode**  
Global Configuration.

**Description**  
Sets up the console IP address, password, mask and gateway.

**Syntax**  
setup

**Sample Output**  
The following example resets the switch and reloads the software.

```
(configure)# setup
Welcome to Switch Setup. The brief series of questions that follows will help you to configure this switch. After completing this process, you will be able to manage the switch using:

- the switch-based HTTP server
- the Element Management System.

Text in [] is the default answer for each questions. To accept the default, press ENTER.

Would you like to change the super user password [Yes]?
.
.
.
```

**Systems**  
**show boot**

**Command Mode**  
User.

**Description**  
Displays BOOT environment information.

**Syntax**  
show boot

**Sample Output**  
The following example displays the boot environment information.

```
> show boot
Checking for valid image in BOOT.
File Information:
File Format Type = Binary
Target Location = Boot
Data Compression = None
Product Information:
Version Number = v2.00.0
Serial Number = 000-00-0000
Model Number = 5500R
Image Information:
Entry Address = 0x00020000
Non-compressed Image:
Size = 0x000779f8 bytes
Checksum = 0xb474
Checksum of image in FEPROM is 0xb474.
Checksum of image in DRAM is 0x9c1f.
.
.
```

**Systems**  
show calendar

Command Mode  User.

Description  Displays the calendar settings.

Syntax  show calendar

Sample Output  The following command displays the calendar settings.

    (configure)# show calendar
    The date is 06/21/2007
    The time is 22:05:34 for Eastern Time (GMT-5)

show clock

Command Mode  User.

Description  Displays the system clock. The [details] option displays the summer-time setting (if any).

Syntax  show clock [details]

Table 30-38. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>details</td>
<td>Display detailed clock information.</td>
</tr>
</tbody>
</table>

Sample Output  The following command show the clock details.

```
(configure)# show clock details
The date is 06/21/2007
The time is 22:04:39 for Eastern Daylight-5)
Summer time hours are in effect
Summer time offset in minutes: 60
Summer time recurring date limits:
    Start - first Sunday of Apr at 02:00
    End   - last Sunday of Oct at 02:00
SNTP client is disabled
```

show cpu

**Command Mode**  
User.

**Description**  
Displays configuration and status information for the supervisor module.

**Syntax**  
show cpu {config | status}

### Table 30-39. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Displays Configuration information for the supervisor modules in slots 1 and 2.</td>
</tr>
<tr>
<td>status</td>
<td>Displays Status information for the supervisor modules in slots 1 and 2.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example displays the cpu configuration information.

```plaintext
> show cpu config
Configuration Information
-------------------------------
Redundant Slot 1 CPU Console Ip Address 0.0.0.0
Redundant Slot 2 CPU Console Ip Address 0.0.0.0
Redundant CPU Default Gateway 0.0.0.0
Switch MAC Prefix 00.30.6D.73.63.ff
Slot 1 Internal IP Address 10.2.2.1
Slot 2 Internal IP Address 0.0.0.0
Internal IP Mask 255.255.255.240
Hello interval 5
```

**Systems**  
show cpu_redundancy

Command Mode User.

Description Displays configuration and status information about the redundant supervisor.

Syntax show cpu_redundancy {config | status}

Sample Output The following example displays the config information for the redundant supervisor slots 1 and 2.

> show cpu_redundancy status

<table>
<thead>
<tr>
<th>Status Information</th>
<th>Slot1 CPU</th>
<th>Slot2 CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Active</td>
<td>N/A</td>
</tr>
<tr>
<td>BOOT Version</td>
<td>v5.00.1</td>
<td>N/A</td>
</tr>
<tr>
<td>Power-Up/Reset Image</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>APP1 Version</td>
<td>b5.00.14</td>
<td>N/A</td>
</tr>
<tr>
<td>APP1 Checksum</td>
<td>0x4be7</td>
<td>N/A</td>
</tr>
<tr>
<td>APP2 Version</td>
<td>x5.00.95</td>
<td>N/A</td>
</tr>
<tr>
<td>APP2 Checksum</td>
<td>0x8cc2</td>
<td>N/A</td>
</tr>
</tbody>
</table>

| Startup Config Date/Time Modified | 00-Dec-06 09:35:25 N/A |
| Startup Config Checksum          | 0x41dc N/A |

<table>
<thead>
<tr>
<th>Statistic Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Reports Sent</td>
<td>0</td>
</tr>
<tr>
<td>Health Reports Received</td>
<td>0</td>
</tr>
<tr>
<td>Health Reports Timeouts</td>
<td>0</td>
</tr>
<tr>
<td>Health Reports Missed</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Synchronization Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No status available.</td>
<td></td>
</tr>
</tbody>
</table>

**show file_name**

**Command Mode** Privileged.

**Description** Displays the contents of a specified file in NVRAM.

**Syntax**

```
show file_name <filename>
```

**Table 30-41. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filename&gt;</td>
<td>The name of a script file in NVRAM. This command works only with filenames that have a &quot;txt&quot; extension. The filename parameters must be in an “8.3” format - one to eight (1-8) character base file name and a required three (3) letter extension.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example displays the contents of the startup.txt file located in NVRAM.

```
# show file_name startup.txt
Documentation# show file_name startup.txt
Contents of file '/NVRAM/startup.txt':
!
! Avaya Switch Agent v5.0.x
!
set intelligent-multicast client-port-pruning enable
set intelligent-multicast client-port-pruning time 60
!
hostname ""
snmp-server location "[Location Not Set]"
snmp-server contact "System Administrator"
clock summer-time recurring 1 Sunday Apr 02:00 5
Sunday Oct 02:00 60
username "root" password encrypted-type1
"$tSfIcnbTP.pxRf7BrhGW31" access-type.
```

show flash

Command Mode User.

Description Displays the layout and contents of flash memory.

Syntax show flash

Sample Output The following example displays the layout and the content of the switch’s flash memory.

> show flash
Checking for valid image in BOOT.
File Information:
    File Format Type = Binary
    Target Location = Boot
    Data Compression = None
Product Information:
    Version Number = v2.00.0
    Serial Number = 000-00-0000
    Model Number = 5500R
Image Information:
    Entry Address = 0x00020000
    Non-compressed Image:
        Size = 0x000779f8 bytes
        Checksum = 0xb474
Checksum of image in FEPROM is 0xb474.
Checksum of image in DRAM is 0x1e12.
.
.

Chapter 30


display running-config

Command Mode  Privileged.

Description  Displays the current running configuration.

Syntax  show running-config

Sample Output  The following example displays the current running configuration.

# show running-config
Current configuration:
! Avaya Switch Agent v5.0.x
! set intelligent-multicast client-port-pruning enable
set intelligent-multicast client-port-pruning time 60
! hostname ""
snmp-server location "[Location Not Set]"
snmp-server contact "System Administrator"
ip http help server "http://199.93.237.91:2010" "help"
clock summer-time recurring 1 Sunday Apr 02:00 5 Sunday
Oct 02:00 60
username "root" password encrypted-type1
"$tSfIcnbTP.pXRf7BrhGW31"
access-type admin
username "diag" password encrypted-type1
"$PQO.vGxkvDhkEDCj2YsoD1"
access-type read-write
username "manuf" password encrypted-type1
"$seHFLP9b16m2v/534Wck90"
access-type read-write
snmp-server community "public" ro normal
.

### show secure-mode

<table>
<thead>
<tr>
<th><strong>Command Mode</strong></th>
<th>User.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Displays the secure mode setting.</td>
</tr>
<tr>
<td><strong>Syntax</strong></td>
<td><code>show secure-mode</code></td>
</tr>
<tr>
<td><strong>Sample Output</strong></td>
<td><code>Secure mode enabled</code></td>
</tr>
<tr>
<td><strong>Systems</strong></td>
<td>P580 and P882.</td>
</tr>
</tbody>
</table>
**show sntp**

**Command Mode**
Global Configuration.

**Description**
Displays information about the Simple Network Time Protocol (SNTP).

**Syntax**
show sntp

**Sample Output**
The following example displays information about the SNTP settings on the switch.

```
(configure)# show sntp
SNTP client is enabled
SNTP server IP address is 199.93.238.247
```

**Systems**
show startup-config

Command Mode  Privileged.

Description  Displays any existing startup configurations (startup.txt file)

Syntax  show startup-config

Sample Output  The following example displays the startup-config.

```
# show startup-config
Documentation# show startup-config
Contents of file '/nvram/startup.txt':
!
! Avaya Inc. Switch Agent v5.0
!
set intelligent-multicast client-port-pruning enable
set intelligent-multicast client-port-pruning time 60
!
hostname ""
snmp-server location "[Location Not Set]"
snmp-server contact "System Administrator"
clock summer-time recurring 1 Sunday Apr 02:00 5 Sunday Oct 02:00 60
username "root" password encrypted-type1
"$tSfIcnbTPlRf7BrhGW31"
  .
  .

show time zone

Command Mode User.

Description Displays a list of time zone abbreviations for use in the clock timezone command.

Syntax show time zone

Sample Output The following example displays the list of time zones set on the switch.

```
(configure)# show time zone
eni        Eniwotok (GMT-12)
kwa        Kwaialien (GMT-12)
im         Midland Island (GMT-11)
haw        Hawaii (GMT-10)
ala        Alaska (GMT-9)
pst        Pacific Time (GMT-8)
ari        Arizona (GMT-7)
mst        Mountain Time (GMT-7)
cst        Central Time USA (GMT-6)
mx         Mexico City (GMT-6)
sac        Saskatchewan (GMT-6)
bog        Bogota (GMT-5)
lim        Lima (GMT-5)
est        Eastern Time (GMT-5)
ind        Indiana (GMT-5)
atl        Atlantic Time (GMT-4)
car        Caracas (GMT-4)
new        Newfoundland (GMT-3:30)
br         Brasilia (GMT-3)
bue        Buenos Aires (GMT-3)
geo        Georgetown (GMT-3)
mat        Mid Atlantic (GMT-2)
--More--
```

show utilization results

Command Mode  User.

Description Displays utilization statistics for the CPU or forwarding engines.

Syntax  show utilization results {{cpu} | {forwarding-engine <chip-fabport> <chip-index>}}


Table 30-42. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu</td>
<td>Displays the CPU utilization statistics</td>
</tr>
<tr>
<td>forwarding-engine</td>
<td>Displays the forwarding engine utilization statistics.</td>
</tr>
<tr>
<td>&lt;chip-fabport&gt;</td>
<td>The fabric port for which you want to view forwarding engine utilization</td>
</tr>
<tr>
<td></td>
<td>statistics.</td>
</tr>
<tr>
<td>&lt;chip-index&gt;</td>
<td>The forwarding engine for which you want to view utilization statistics.</td>
</tr>
</tbody>
</table>

Sample Output  >  show utilization results cpu

Average CPU Utilization over the 60 second sample window: 0 percent

Individual Sample Utilizations (sorted from most recent to oldest):
Sample 0: 2 percent
Sample 1: 2 percent
Sample 2: 2 percent
Sample 3: 5 percent
Sample 4: 3 percent
Sample 5: 2 percent
Sample 6: 2 percent
Sample 7: 2 percent
Sample 8: 3 percent
Sample 9: 3 percent
Sample 10: 2 percent
Sample 11: 3 percent

Systems  P580 and P882.
show utilization settings

Command Mode  User.

Description  Displays the current settings for utilization monitoring.

Syntax  show utilization settings

Sample Output  CPU monitoring is enabled
Forwarding Engine monitoring is enabled

CPU threshold level is 95 percent
Forwarding Engines:
FIRE threshold level is 95 percent
FORE threshold level is 95 percent

CPU threshold event generation is enabled
Forwarding Engine threshold event generation is enabled

Systems  P580 and P882.
show version

Command Mode User.

Description Displays the software version currently running on the switch.

Syntax show version

Sample Output The following example displays the software version currently running on
the switch.

> show version
Avaya Switch Agent v5.3.1

Overview

This chapter describes the following commands:

- clear temperatures
- set temperature (shutdown)
- set temperature (warning)
- show temperatures
clear temperatures

Command Mode

Global Configuration.

Description

Resets all configured warning and shutdown temperatures (in Celsius) to their default values. The default values are listed in Table 31-1.

Syntax

clear temperatures

Sample Output

The following example resets all configured warning and shutdown temperatures to their default settings.

(configure)# clear temperatures

Systems


Table 31-1. Default Shutdown and Warning Temperatures

<table>
<thead>
<tr>
<th>Component</th>
<th>Shutdown</th>
<th>Upper Warning</th>
<th>Lower Warning</th>
<th>Low Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Sensor</td>
<td>100°</td>
<td>85°</td>
<td>5°</td>
<td>0°</td>
</tr>
<tr>
<td>All others</td>
<td>65°</td>
<td>60°</td>
<td>5°</td>
<td>0°</td>
</tr>
</tbody>
</table>
set temperature (shutdown)

Command Mode  Global Configuration.

Description  Sets the shutdown temperature for a specific component of the switch. The default setting for the CPU sensor is 100° C. The default setting for all other components is 65°C.

Syntax  

```
set temperature {supervisor-slot | backplane-sensor | cpu-sensor | probe} shutdown <temperature>
```

Sample Output  

The following example sets the CPU sensor shutdown temperature to 95° (Celsius).

```
(configure)# set temperature shutdown cpu-sensor 95
```

Systems  


Table 31-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| {supervisor-slot | backplane-sensor | cpu-sensor | probe}             | Indicates which component of the switch you are setting the shutdown temperature for.  
**Note:** After you change the temperature settings for the active supervisor, you must synchronize the active and standby supervisors to copy the temperature settings to the standby supervisor. |
| shutdown              | Shutdown is a required parameter and indicates that the shutdown limit temperature is being set. |
| <temperature>         | Temperature is a required parameter and when the switch measures this value on this component, it shuts itself down to prevent either inconsistent behavior or damage to itself or surrounding equipment.  
The command checks the entered temperature value and ensures that the temperature being set is not above 127, and not below -128 degrees, the backplane sensor and supervisor are not below 60 and not above 127 degrees, and the CPU sensor is not below 85 and not above 127 degrees. |
set temperature (warning)

**Command Mode**
Global Configuration.

**Description**
Sets the warning temperature (in Celsius) for a specific component of the switch. The default values are listed in Table 31-3.

**Syntax**
```
set temperature {supervisor-slot | backplane-sensor | cpu-sensor | probe} warning {upper | lower | low-limit} <temperature>
```

**Table 31-3. Default Warning Temperatures**

<table>
<thead>
<tr>
<th>Component</th>
<th>Upper Warning</th>
<th>Lower Warning</th>
<th>Low Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Sensor</td>
<td>85°</td>
<td>5°</td>
<td>0°</td>
</tr>
<tr>
<td>All others</td>
<td>60°</td>
<td>5°</td>
<td>0°</td>
</tr>
</tbody>
</table>

**Table 31-4. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| {supervisor-slot | backplane-sensor | cpu-sensor | probe} | Indicates which component of the switch you are setting the temperature for.  
**Note:** After you change the temperature settings for the active supervisor, you must synchronize the active and standby supervisors to copy the temperature settings to the standby supervisor. |
| warning         | Required parameter indicating that a warning limit is being modified.                                                                          |
### Table 31-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{upper</td>
<td>lower</td>
</tr>
<tr>
<td></td>
<td>Upper warning:</td>
</tr>
<tr>
<td></td>
<td>• Backplane is 5 to 65 degrees</td>
</tr>
<tr>
<td></td>
<td>• CPU is 5 to 100 degrees</td>
</tr>
<tr>
<td></td>
<td>• Supervisor Module is 5 to 65 degrees.</td>
</tr>
<tr>
<td></td>
<td>Lower warning:</td>
</tr>
<tr>
<td></td>
<td>• Backplane is -128 to 5 degrees</td>
</tr>
<tr>
<td></td>
<td>• CPU is degrees 0 to 100</td>
</tr>
<tr>
<td></td>
<td>• Supervisor Module is 0 to 65 degrees.</td>
</tr>
<tr>
<td></td>
<td>Low- limit:</td>
</tr>
<tr>
<td></td>
<td>• Backplane is -128 to +5 degrees</td>
</tr>
<tr>
<td></td>
<td>• CPU is -128 to +100 degrees</td>
</tr>
<tr>
<td></td>
<td>• Supervisor Module is -128 to +65 degrees.</td>
</tr>
<tr>
<td>&lt;temperature&gt;</td>
<td>Temperature in degrees Celsius for the warning.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example sets the backplane-sensor upper warning temperature to 44° (Celsius).

```
(configure)# set temperature backplane-sensor warning upper 44
```

**Systems**

show temperatures

**Command Mode**  
User.

**Description**  
Displays the current temperatures and the configured temperature limits. There is no reverse mapping to this command.

**Syntax**  
show temperatures

**Sample Output**  
The following example displays the current switch temperatures.

```
> show temperature

<table>
<thead>
<tr>
<th></th>
<th>Slot 2 Sensor</th>
<th>Backplane Sensor</th>
<th>CPU Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutdown (C)</td>
<td>65</td>
<td>65</td>
<td>100</td>
</tr>
<tr>
<td>Upper Warning (C)</td>
<td>60</td>
<td>60</td>
<td>85</td>
</tr>
<tr>
<td>Current</td>
<td>27</td>
<td>29</td>
<td>24</td>
</tr>
<tr>
<td>Lower Warning (C)</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Low Limit (C)</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Systems**  
Overview

This chapter describes the following commands:

- configure
- connect
- custom-access-type
- disable
- enable
- end
- exit
- help
- length
- password
- set custom-access-type
- set debug
- set login
- show custom-access-type
- show history
- show login
- show sessions
- show username
- telnet
- terminal databits
- terminal flowcontrol
- terminal length
- terminal output pause
- terminal parity
- terminal speed
- terminal stopbits
- terminal width
- username
- width
configure

Command Mode  Privileged.

Description  Enters the Global Configuration mode.

Syntax  configure

Sample Output  The following example enters Global Configuration mode on the switch CLI:

    # configure
    (configure)#

connect

Command Mode       Privileged.
Description         Log in to a host that supports Telnet.
Syntax              `connect { <ip-addr> | <hostname> }`

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;ip-addr&gt;</code></td>
<td>The IP address of the host in 4-part, dotted-decimal notation.</td>
</tr>
<tr>
<td><code>&lt;hostname&gt;</code></td>
<td>The name of the host.</td>
</tr>
</tbody>
</table>

Sample Output    The following example connects to the host with the IP address 123.23.23.2.
# connect 123.23.23.2

# custom-access-type

**Command Mode**  
Global Configuration.

**Description**  
Creates a custom access type. The switch supports a maximum of 30 custom access types.

## Syntax

<table>
<thead>
<tr>
<th>To Create:</th>
<th>custom-access-type &lt;catName&gt; [sys-configuration [ro]] [module-port-mgmt [ro]] [events-mgmt [ro]] [l2-switching [ro]] [routing [ro]]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Delete:</td>
<td>no custom-access-type &lt;catName&gt;</td>
</tr>
</tbody>
</table>

## Table 32-2. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;catName&gt;</td>
<td>The name of the custom access type. You can enter up to 31 characters. Do not use spaces.</td>
</tr>
<tr>
<td>[sys-configuration]</td>
<td>Allows users to access system configuration settings. If you do not enter this option, users who are assigned to the custom access type cannot access system configuration settings.</td>
</tr>
<tr>
<td>[ro]</td>
<td>Enables read-only permission. If you do not enter this option, users who are assigned to the custom access type have read-write permission for the feature.</td>
</tr>
<tr>
<td>[module-port-mgmt]</td>
<td>Allows users to access module and port settings. If you do not enter this option, users who are assigned to the custom access type cannot access module and port settings.</td>
</tr>
<tr>
<td>[events-mgmt]</td>
<td>Allows users to access event settings. If you do not enter this option, users who are assigned to the custom access type cannot access event settings.</td>
</tr>
</tbody>
</table>
Table 32-2. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[l2-switching]</td>
<td>Allows users to access layer 2 switching settings. If you do not enter this option, users who are assigned to the custom access type cannot access layer 2 switching settings.</td>
</tr>
<tr>
<td>[routing]</td>
<td>Allows users to access routing settings. If you do not enter this option, users who are assigned to the custom access type cannot access routing settings.</td>
</tr>
</tbody>
</table>

Sample Output

For example, the following command creates a custom access type that allows users read-only permission for module and port settings and read-write permission for layer 2 switching settings:

```
(configure)# custom-access-type CAT1 module-port-mgmt ro l2-switching
```

Users who are assigned to the CAT1 custom access type cannot view or modify settings for system configuration, events, or routing.

Systems

P580 and P882.
### disable

**Command Mode**  
Privileged.

**Description**  
Exits Privileged mode. Returns to User mode.

**Syntax**  
disable

**Sample Output**  
The following example exits Privileged mode.

```
# disable
```

**Systems**  
enable

**Command Mode**
User.

**Description**
Enteres the Privileged mode.

**Syntax**
`enable`

**Sample Output**
The following example enters Privileged mode:

```
> enable
#
```

**Systems**
end

**Command Mode**  
Global Configuration.

**Description**  
Exits Global Configuration mode and returns to Privileged mode.

**Syntax**  
end

**Sample Output**  
The following example exits Global Configuration mode.

```
(configure)# end
#
```

**Systems**  
exit

Command Mode  All modes.

Description  Exits the current mode and reenters the previous mode.

Syntax  exit

Sample Output  The following example exits Global Configuration mode.

    (configure) # exit

    #

help

Command Mode  User.

Description  Displays a list of commands that are available in the current command mode and a brief description of each command.

Syntax  help

Sample Output  This example displays the commands that are available in User mode.

> help
dir [<filename>]
  Displays the list of files in NVRAM, or a specific filename
enable
  Enter privileged mode
exit
  Exit current mode and re-enter previous mode
help
  Display full help list of all commands available in the current mode
ip mtrace
no ip mtrace
  enable/disable mtrace globally.
legacy-cli
  Enter Legacy CLI Mode
.
.

length

Command Mode  User.

Description  Sets the terminal screen length. The default value is 24. Use the no form of this command to restore the default value of 24.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>length &lt;length&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no length</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the number of lines to print to 50:

> length 50


Table 32-3. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;length&gt;</td>
<td>The number of lines to print before displaying the --more-- prompt (5+ Lines).</td>
</tr>
</tbody>
</table>
password

Command Mode User.

Description Changes a user password. All users can change their own passwords.

Syntax password <passwd>

Table 32-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;passwd&gt;</td>
<td>A new password. Passwords can consist of a maximum of 31 characters.</td>
</tr>
<tr>
<td></td>
<td>Do not use a combination of the following special characters for the password ;, ?, , , #, $, %, ^, &amp;, or *.</td>
</tr>
</tbody>
</table>

Systems P580 and P882.
**set custom-access-type**

**Command Mode**  
Global Configuration.

**Description**  
Modifies an existing custom-access-type.

**Syntax**  
```
set custom-access-type <catName> [sys-configuration {ro | rw | none}] [module-port-mgmt {ro | rw | none}] [events-mgmt {ro | rw | none}] [lswitching {ro | rw | none}] [routing {ro | rw | none}]
```

*Note:* Unlike the `custom-access-type` command that you use to create a custom access type, you must specify read-only, read-write, or no permission when you use the `set custom-access-type` command to modify a custom access type.

**Table 32-5. Keywords, Arguments, and Options**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;catName&gt;</code></td>
<td>The name of the custom access type that you want to modify.</td>
</tr>
<tr>
<td>[sys-configuration]</td>
<td>Changes the permission for system configuration settings. If you do not enter this option, the current permission is retained.</td>
</tr>
<tr>
<td>{ro</td>
<td>rw</td>
</tr>
<tr>
<td>[module-port-mgmt]</td>
<td>Changes the permission for module and port settings. If you do not enter this option, the current permission is retained.</td>
</tr>
<tr>
<td>[events-mgmt]</td>
<td>Changes the permission for event settings. If you do not enter this option, the current permission is retained.</td>
</tr>
</tbody>
</table>
Sample Output

For example, the following command gives custom access type CAT1 read-write permission for module and port settings and read-only permission for system configuration settings:

```
(configure)# custom-access-type CAT1 sys-configuration ro module-port-mgmt rw
```

The permissions for all other features are unchanged.

Systems

P580 and P882.
set debug

Command Mode  
Global Configuration.

Description  
Enables or disables debug mode. If enabled, this mode displays system messages that help Avaya Technical Support troubleshoot network problems.

* Important:  Avaya recommends that debug mode be enabled only during troubleshooting sessions. If debug mode is enabled during normal network operation, the switch may display messages that users incorrectly interpret as indications of system failures. For more information on advanced troubleshooting, see User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1.

By default, this mode is disabled.

Syntax  
set debug {on | off}

Table 32-6. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables debug mode.</td>
</tr>
<tr>
<td>off</td>
<td>Disables debug mode.</td>
</tr>
</tbody>
</table>

Systems  
set login

Command Mode  Global Configuration.

Description  Configures user account security.

Syntax  set login [attempts <num-login-attempts>] [timeout-limit <timeout-limit>] [min-password-length <min-password-length>]

Table 32-7. Keywords, Arguments, and Options

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;num-login-attempts&gt;</td>
<td>Number of login attempts that you want to allow users. When a user exceeds the limit for login attempts, his or her user account is disabled and the switch displays an error message. Valid values for this field are 3 to 99 login attempts.</td>
</tr>
<tr>
<td>&lt;timeout-limit&gt;</td>
<td>Number of seconds that you want a user account disabled when the limit for login attempts is exceeded. Once the timeout limit expires, the user can attempt to login again.</td>
</tr>
<tr>
<td>&lt;min-password-length&gt;</td>
<td>Minimum number of characters that you want to allow for user passwords. If a user attempts to create a password with fewer characters, the switch displays the following error message: Password too short – must be at least &lt;x&gt; characters.</td>
</tr>
</tbody>
</table>

Systems  P580 and P882.
show custom-access-type

Command Mode  User.

Description  Displays the custom access types that are currently configured on the switch.

Syntax  show custom-access-type

Systems  P580 and P882.
### show history

**Command Mode**  
User.

**Description**  
Displays an alphabetic list of the last 20 commands entered in the current session.

**Syntax**  
show history

**Sample Output**  
The following example displays the last commands entered in the current session:

```plaintext
> show history
show appletalk nbp
show appletalk route
show appletalk traffic
show appletalk zone
show boot
show buffering fabric-port
show buffering fabric-port
.
.
```

**Systems**  
show login

Command Mode
Privileged.

Description
Displays the current settings for user account security. The following settings are displayed:

- Login attempt limit
- Timeout limit
- Minimum password length

Syntax
show login

Sample Output
Login attempt limit:    3
Timeout limit:         60 seconds
Minimum password length: 0 characters

Systems
P580 and P882.
show sessions

Command Mode: User.

Description: Displays the active Telnet, serial, and PPP CLI sessions.

Syntax: show sessions

Sample Output: The following example displays the active sessions:

```
> show sessions
Session ID  Line ID  Location
 1          6vty     205.181.0.56:yyyy
```

show username

Command Mode User.

Description Displays user account settings. The following information is displayed for each user account:

- User name
- Access type
- Management type
- Expiration date
- Status

Syntax username [<name>]

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>The user account for which you want to view settings. If you do not enter this option, all user accounts are displayed.</td>
</tr>
</tbody>
</table>

Sample Output

<table>
<thead>
<tr>
<th>User Name</th>
<th>Access Type</th>
<th>Management Type</th>
<th>Exp Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>Administrator</td>
<td>All</td>
<td>-</td>
<td>Enable</td>
</tr>
<tr>
<td>diag</td>
<td>Diagnostic</td>
<td>All</td>
<td>-</td>
<td>Enable</td>
</tr>
<tr>
<td>manuf</td>
<td>Manufacturing</td>
<td>All</td>
<td>-</td>
<td>Enable</td>
</tr>
<tr>
<td>nm</td>
<td>Read-write</td>
<td>All</td>
<td>12-31-2003</td>
<td>Enable</td>
</tr>
<tr>
<td>bob</td>
<td>Read-only</td>
<td>Remote-CLI, Web</td>
<td>8-31-2004</td>
<td>Enable</td>
</tr>
<tr>
<td>bill</td>
<td>Administrator</td>
<td>All</td>
<td>-</td>
<td>Enable</td>
</tr>
</tbody>
</table>

Systems P580 and P882.
**telnet**

**Command Mode**  
Privileged.

**Description**  
Starts a Telnet session to the host that you specify.

**Syntax**  
telnet {<ip-address> | <host-name>} [<tcp-port>]

**Table 32-9. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip-address&gt;</td>
<td>The IP address of the host to which you want to start a Telnet session.</td>
</tr>
<tr>
<td>&lt;hostname&gt;</td>
<td>The DNS host name of the host to which you want to start a Telnet session.</td>
</tr>
<tr>
<td>[&lt;tcp-port&gt;]</td>
<td>The TCP port number for Telnet requests.</td>
</tr>
<tr>
<td></td>
<td>You need to enter this parameter only if the TCP port for Telnet is set to a port number other than 23.</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example starts a Telnet session to the switch at 192.161.55.83:

```
# telnet 192.161.55.83
translating 192.161.55.83...ok
connecting to host 192.161.55.83
(192.161.55.83)...open
escape character is ‘^]’
type ‘^] c’ to close Telnet Connection
Login:
```

The following example starts a Telnet session to the switch at 192.168.0.126. The switch is set to use TCP port 9998 for Telnet requests:

```
# telnet 192.168.0.126 9998
```

**Systems**  
**terminal databits**

**Command Mode**
Global Configuration.

**Description**
Sets the databits width on the terminal port (also called console port).

**Syntax**
```
terminal databits {7 | 8}
```

**Table 32-10. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{7</td>
<td>8}</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the terminal databits width to 8:

```
(configure)# terminal databits 8
```

**Systems**
terminal flowcontrol

Command Mode  Global Configuration.

Description  Sets the flow control for the terminal port (also called console port).

Syntax  terminal flowcontrol {none | xon/xoff}

Table 32-11. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{none</td>
<td>xon/xoff}</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the terminal flowcontrol parameter to xon/xoff:

(configure)# terminal flowcontrol xon/xoff

### terminal length

**Command Mode**
User, Privileged, or Global Configuration.

**Description**
Sets the number of lines on the terminal screen for the current session. The `no` form of this command restores the default length to 24 lines.

**Syntax**

<table>
<thead>
<tr>
<th>To Set:</th>
<th>terminal length <code>&lt;length&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] terminal length</td>
</tr>
</tbody>
</table>

**Table 32-12. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;length&gt;</code></td>
<td>The number of lines to print before displaying the <code>--more--</code> prompt (5+ Lines).</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example sets the number of lines on the terminal screen for the current session to 50:

```
> terminal length 50
```

**Systems**
terminal output pause

**Command Mode**  
User.

**Description**  
Enables output from the terminal to pause when the configured screen length is reached. A pause is indicated by a `--more--` prompt. The no form of this command disables this function.

In addition, you can terminate a current print job by pressing Control + C at the `--more--` prompt. Continue printing by pressing either Enter or the Spacebar.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>terminal output pause</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no terminal output pause</td>
</tr>
</tbody>
</table>

**Sample Output**  
The following example disables the terminal output pause function:

```plaintext
> no terminal output pause
```

**Systems**  
terminal parity

Command Mode  Global Configuration.

Description  Sets the parity parameter on the console port.

Syntax  terminal parity {none | even | odd}

Sample Output  The following example sets the terminal parity parameter to none:

(configure)# terminal parity none

Table 32-13. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{none</td>
<td>even</td>
</tr>
</tbody>
</table>

terminal speed

Command Mode  Global Configuration.

Description  Sets the baud rate on the console port. The default baud rate is 9600.

Syntax  terminal speed {300 | 1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}

Sample Output  The following example sets the terminal speed to 19200:

    (configure)# terminal speed 19200


Table 32-14. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>300</td>
<td>1200</td>
</tr>
</tbody>
</table>
terminal stopbits

Command Mode  Global Configuration.

Description  Sets the stopbits parameter on the console port.

Syntax  terminal stopbits {1 | 2}

Sample Output  The following example sets the terminal stopbits to 1:

(configure)# terminal stopbits 1

Table 32-15. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>{1</td>
<td>2}</td>
</tr>
</tbody>
</table>

terminal width

Command Mode  User.

Description  Sets the number of character columns on the terminal screen. The no form of this command restores the default value of 80 characters.

Syntax

<table>
<thead>
<tr>
<th>To Set:</th>
<th>terminal width &lt;characters&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no terminal width</td>
</tr>
</tbody>
</table>

Table 32-16. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;characters&gt;</td>
<td>The screen width (40+ characters).</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the terminal width to 120 characters:

> terminal width 120

username

Command Mode          Privileged.

Description          Creates a new user account. You can create up to 27 user accounts.

Syntax

<table>
<thead>
<tr>
<th>Operation</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Create:</td>
<td>username &lt;name&gt; password [encrypted-type1] &lt;passwd&gt; [access-type {read-only</td>
</tr>
<tr>
<td>To Delete:</td>
<td>no username &lt;name&gt;</td>
</tr>
<tr>
<td>To Set Expiration Period</td>
<td>username &lt;name&gt; [exp-period &lt;exp-period&gt;] [exp-warning &lt;exp-warning&gt;]</td>
</tr>
<tr>
<td>and Expiration Warning</td>
<td></td>
</tr>
<tr>
<td>To Enable or Disable:</td>
<td>username &lt;name&gt; status {enable</td>
</tr>
</tbody>
</table>

Table 32-17. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>The user name that you want to create. User names can consist of a maximum of 31 characters.</td>
</tr>
<tr>
<td>[encrypted-type1]</td>
<td>Indicates that user password is an MD5-encrypted string. If you enter the [encrypted-type1] option, you must enter an MD5-encrypted string for the &lt;passwd&gt; argument.</td>
</tr>
<tr>
<td>&lt;passwd&gt;</td>
<td>The password for the user name. Passwords can consist of a maximum of 31 characters.</td>
</tr>
<tr>
<td>Note:</td>
<td>Do not use a combination of the following special characters for the password ;, ?, , ,#, $, %, ^, &amp;, or *.</td>
</tr>
</tbody>
</table>
Table 32-17. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
</table>
| [access-type {read-only | read-write | admin | <catName>}]) | The access type for the user. Options are:  
  - read-only  
  - read-write  
  - admin  
  - <catName>  
  The <catName> variable assigns a custom access type to the user. For information about custom access types, see Chapter 2, “Setting Up the Switch,” in the User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1. The default access type is read-only. |
| [mgmt-type [all] [local-cli] [remote-cli] [web]] | The management interfaces to which you want the user to have access. Options are:  
  - all—All management interfaces.  
  - local-cli—CLI on the PC that is connected to the serial port on the supervisor module.  
  - remote-cli—CLI by means of a Telnet connection.  
  - web—Web Agent.  
  The default setting is all. |
| <exp-period> | Number of weeks for which the user account is valid. The expiration period can range from 3 to 999 weeks. The default setting is 0, no expiration.  
  When a user account expires, you must reset the account.  
  Use the username <name> status {enable | disable} command to reset the account. |
| <exp-warning> | Number of weeks before user account expiration that you want the user warned. The expiration warning can range from 0 to the expiration period. A setting of 0 indicates that no warning is generated. |
| enable | Enables the user account. |
| disable | Disables the user account. |

Sample Output

The following example creates the username *boston* with a password of *mass* and an access-type of admin:

```
# username boston password mass access-type admin
```

Systems

P580 and P882.
**width**

**Command Mode** User.

**Description** Sets the number of character columns on the terminal screen. The **no** form of this command restores the default value of 80 characters.

**Syntax**

<table>
<thead>
<tr>
<th>To Set:</th>
<th>width &lt;width&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>no width</td>
</tr>
</tbody>
</table>

**Table 32-18. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;width&gt;</td>
<td>The screen width (40+) characters.</td>
</tr>
</tbody>
</table>

**Sample Output** The following example sets the number of character columns on the terminal screen to 50:

```
> width 50
```

Overview

This chapter describes:

- set 3com-mapping-table
- set vlan
- set vlan (frame format)
- set vlan <vlan-id> <mod-swport-range>
- set vtp-snooping domain
- show 3com-mapping-table
- show vlan
- show vtp-snooping configure
set 3com-mapping-table

Global Configuration.

Description
Creates or deletes a 3Com mapping table.

Syntax

| To Configure: | set 3com-mapping-table <table-name>  
[...table-entry <entry-num> vlan {<vlan-id> |  
name <vlan-name>} [,] ] |
| To Delete: | clear 3com-mapping-table <table-name>  
[... table-entry <entry-num> [,] ] |

Table 33-1. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;table-name&gt;</td>
<td>The name of the mapping table to be deleted.</td>
</tr>
<tr>
<td>&lt;entry-num&gt;</td>
<td>The entry number in the table.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>Specifies a VLAN by its VLAN ID.</td>
</tr>
<tr>
<td>&lt;name-name&gt;</td>
<td>Specifies a VLAN by its name.</td>
</tr>
</tbody>
</table>

Sample Output
The following example clears an entry from a 3Com mapping table.

(configure)# clear 3com-mapping-table TestTable table-entry 2
Entry (tag) 2 in table "TestTable" was successfully cleared

Systems
set vlan

**Command Mode**
Global Configuration.

**Description**
Creates a VLAN or modifies the name of an existing VLAN. The `clear` command deletes a VLAN.

If the VLAN that you specify does not exist, this command creates the VLAN. If the VLAN that you specify does exist, this command renames the VLAN and ignores any optional arguments that you enter.

| To Configure: | set vlan `<vlan-id>` [name `<vlan-name>`] [autoincrement-HT-size {true | false}] [init-HT-size `<size>`] |
|---------------|--------------------------------------------------------------------------------------------------|
| To Delete:    | clear vlan `{<vlan-id> | name `<vlan-name>`}`                                                                |

**Table 33-2. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vlan-id&gt;</code></td>
<td>The VLAN ID.</td>
</tr>
<tr>
<td>[name <code>&lt;vlan-name&gt;</code>]</td>
<td>The VLAN name.</td>
</tr>
<tr>
<td>[autoincrement-HT-size {true</td>
<td>false}]</td>
</tr>
<tr>
<td>[init-HT-size <code>&lt;size&gt;</code>]</td>
<td>Specifies the initial hash table size. The table size can be 16, 32, 64, 128, 256, 512, 1024, 2048, 4096 or 8192. The default setting is 1024.</td>
</tr>
</tbody>
</table>

**Systems**
set vlan (frame format)

**Command Mode**
Global Configuration.

**Description**
Modifies the frame tagging format of the specified switch ports that are bound to the specified VLAN.

**Syntax**
```
set vlan {<vlan-id> | name <vlan-name>} <mod-swport-range> [...,<mod-swport-range>] frame-format {clear | from-port}
```

**Table 33-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vlan-id&gt;</code></td>
<td>The VLAN that the switch port is bound to by its VLAN ID.</td>
</tr>
<tr>
<td><code>&lt;vlan-name&gt;</code></td>
<td>The VLAN the switch port is bound to by its name.</td>
</tr>
<tr>
<td><code>&lt;mod-swport-range&gt;</code></td>
<td>A single switch port or range of switch ports on a module.</td>
</tr>
</tbody>
</table>
| frame-format `{clear | from-port}` | • **clear** means frames sent out the specified ports in the specified VLAN are sent out without tags, regardless of what the trunking attribute of the switch ports is set to.  
  • **from-port** means that the frames are sent out with whatever tag the switch ports trunking attribute is set to, if any. |

**Sample Output**
The following example sets the frame format for vlan 1 4/1 to clear:

```
(configure)# set vlan 1 4/1 frame-format clear
VLAN ID 1, switch port 4/1 frame-format set to "clear"
```

**Systems**
**set vlan <vlan-id> <mod-swport-range>**

**Command Mode**
Global Configuration.

**Description**
Binds additional ports to a VLAN if trunking is enabled on the specified port. Non-trunk ports support only a single, default VLAN per port. Binding multiple VLANs to a non-trunk port is NOT recommended and can have adverse effects on network performance. To set the single, default VLAN for a non-trunk port, use the `set port vlan` command.

All untagged frames are forwarded to the default VLAN, which you use the `set port vlan` command to set. All tagged frames are forwarded to the VLAN indicated by the tag.

* **Note:** If automatic VLAN creation is disabled on an:
  - 80-series port, packets tagged for a VLAN that does not exist on the switch are dropped.
  - 50-series port, packets tagged for a VLAN that does not exist on the switch are forwarded to the default VLAN.

For more information on the relationship between the settings for trunk mode, automatic VLAN creation, and VLAN binding, see Chapter 8, “Configuring Ports,” of *User Guide for the Avaya P580 and P882 Multiservice Switches, Software Version 6.1*.

When you use the `set vlan {<vlan-id> | name <vlan-name>} <mod-swport-range>` command to bind multiple VLANs to a port, the port becomes part of the flooding domain of the selected VLAN. This command provides an alternative to using the binding types `bind to all` and `bind to receive` that makes it possible for you to add ports to a subset of VLANs on the switch.

* **Important:** This configuration may cause undesirable results, for example, destination unicast storms, and should be used only under special circumstances and only with the assistance of customer support.

**Syntax**

| To Bind Ports:                     | `set vlan {<vlan-id> | name <vlan-name>} <mod-swport-range>[,...,<mod-swport-range>]` |
|------------------------------------|---------------------------------------------------------------------------|
| To Remove Ports:                   | `clear vlan {<vlan-id> | name <vlan-name>} <mod-swport-range>[,...,<mod-swport-range>]` |
Sample Output

In the following example, 5/1 refers to port 1 on module 5. 5/1-20 refers to ports 1 through 20 on module 5. This command also accepts a comma-delimited list of ports or port ranges.

```
(configure)# set vlan 100 4/1, 4/3-4
WARNING: Port 4.1 is being bound to a VLAN other than the default VLAN when trunking format of the port is set to Clear
Switch port 4/1 bound to VLAN ID 100
WARNING: Port 4.3 is being bound to a VLAN other than the default VLAN when trunking format of the port is set to Clear
Switch port 4/3 bound to VLAN ID 100
WARNING: Port 4.4 is being bound to a VLAN other than the default VLAN when trunking format of the port is set to Clear
Switch port 4/4 bound to VLAN ID 100
```

```
(configure)# clear vlan 100 4/1, 4/3-4
Switch port 4/1 unbound from VLAN ID 100
Switch port 4/3 unbound from VLAN ID 100
Switch port 4/4 unbound from VLAN ID 100
```

**Systems**


---

### Table 33-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The VLAN ID to add or remove ports to or from.</td>
</tr>
<tr>
<td>[name &lt;vlan-name&gt;]</td>
<td>The VLAN to add or remove ports to or from.</td>
</tr>
<tr>
<td>&lt;mod-swport-range&gt;</td>
<td>A single switch port or range of switch ports on a module.</td>
</tr>
</tbody>
</table>
set vtp-snooping domain

**Command Mode**
Global Configuration.

**Description**
Defines the VTP domain name from which the switch learns VLANs from Cisco VTP frames. The **clear** form of this command clears any learned or defined domain name. The default setting is a null string.

If VTP snooping is globally enabled and you do not set a VTP domain name, the switch automatically learns the domain name from the Cisco VTP server.

**Syntax**

<table>
<thead>
<tr>
<th>To Define:</th>
<th>set vtp-snooping domain <code>&lt;vtp-domain-name&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Clear:</td>
<td>clear vtp-snooping domain</td>
</tr>
</tbody>
</table>

**Table 33-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vtp-domain-name&gt;</code></td>
<td>The Cisco VTP domain name to which this switch listens for VTP messages.</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example set the VTP snooping domain name to Corporate.

```
(configure)# set vtp-snooping domain Corporate
vtp-snooping parameter modified.
```

**Systems**
**show 3com-mapping-table**

**Command Mode**  
User.

**Description**  
Displays the 3Com mapping tables. All tables are displayed by default.

**Syntax**  
```
show 3com-mapping-table [table-name]
```

**Sample Output**  
The following example shows the 3Com Mapping Table for the switch.

```
> show 3com-mapping-table
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[table-name]</td>
<td>The name of the 3Com mapping table. If not included, this command will display all of the tables configured on the switch.</td>
</tr>
</tbody>
</table>

---

Table Name: “3ComDefault”
Table Entries: [entry num: vlan name (vlan id)]

<table>
<thead>
<tr>
<th>1: Default (1)</th>
<th>2:Discard (4097)</th>
<th>3: Discard (4097)</th>
<th>4:Discard(4097)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5: Discard (4097)</td>
<td>6: Discard (4097)</td>
<td>7: Discard (4097)</td>
<td>8: Discard(4097)</td>
</tr>
<tr>
<td>9: Discard (4097)</td>
<td>10:Discard (4097)</td>
<td>11: Discard(4097)</td>
<td>12: Discard(4097)</td>
</tr>
<tr>
<td>13: Discard (4097)</td>
<td>14:Discard(4097)</td>
<td>15:Discard (4097)</td>
<td>16: Discard(4097)</td>
</tr>
</tbody>
</table>

---

**Systems**  
show vlan

Command Mode
User.

Description
Displays information about all VLANs on the switch or the VLAN that you specify.

Syntax

<table>
<thead>
<tr>
<th>To Display All VLANs:</th>
<th>show vlan [detailed]</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Display One VLAN:</td>
<td>show vlan {&lt;vlan-id&gt;</td>
</tr>
</tbody>
</table>

Table 33-7. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>[detailed]</td>
<td>Shows a detailed output of the VLANs that currently exist on the system including switch ports that are bound to that VLAN.</td>
</tr>
<tr>
<td>&lt;vlan-id&gt;</td>
<td>The VLAN ID.</td>
</tr>
<tr>
<td>[name &lt;vlan-name&gt;]</td>
<td>The VLAN name.</td>
</tr>
</tbody>
</table>

Sample Output
The following example displays detailed information about the VLANs currently configured on the switch.

(configure)# show vlan detailed

<table>
<thead>
<tr>
<th>ID</th>
<th>VLAN Name</th>
<th>Group ID</th>
<th>AFT Index</th>
<th>Learned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Default</td>
<td>2</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>*autoVlan2</td>
<td>4</td>
<td>9</td>
<td>Aut</td>
</tr>
<tr>
<td>10</td>
<td>jerry2</td>
<td>10</td>
<td>10</td>
<td>-</td>
</tr>
<tr>
<td>20</td>
<td>jerry3</td>
<td>20</td>
<td>11</td>
<td>-</td>
</tr>
<tr>
<td>25</td>
<td>*autoVlan25</td>
<td>25</td>
<td>12</td>
<td>Aut</td>
</tr>
<tr>
<td>30</td>
<td>*autoVlan30</td>
<td>30</td>
<td>13</td>
<td>Aut</td>
</tr>
<tr>
<td>50</td>
<td>*autoVlan50</td>
<td>50</td>
<td>14</td>
<td>Aut</td>
</tr>
<tr>
<td>4097</td>
<td>Discard</td>
<td>3</td>
<td>3</td>
<td>-</td>
</tr>
</tbody>
</table>

Systems
show vtp-snooping configure

Command Mode User.

Description Displays the configured and learned VTP snooping configuration information. The default is None.

Syntax show vtp-snooping configuration

Sample Output The following example displays vtp-snooping configuration information.

```
(configure)# show vtp-snooping configuration
VTP Snooping State: Enable
Domain Name: Corporate
Configuration Revision Number: 28
Updater Identity: 199.160.0.140
Update Timestamp: 99/10/05.10:02:50
```

Overview

This chapter describes:

- router vrrp
- ip vrrp
- ip vrrp (vr-id)
- ip vrrp (auth-key)
- ip vrrp (override)
- ip vrrp (preempt)
- ip vrrp (priority)
- ip vrrp (timer)
- show ip vrrp
**router vrrp**

**Command Mode**
Global Configuration.

**Description**
Enables and disables VRRP routing globally. Use the **no** form of this command to disable VRRP routing.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>router vrrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no router vrrp</td>
</tr>
</tbody>
</table>

**Sample Output**
The following example enables vrrp globally.

```
(configure)# router vrrp
```

**Systems**
**ip vrrp**

**Command Mode** Interface Configuration.

**Description** Enables or disables VRRP (Virtual Router Redundancy Protocol) on an interface. Use the `no` form of this command to disable VRRP on an interface.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip vrrp</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip vrrp</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example enables VRRP on an interface labeled `boston`.

```
(config-if:boston)# ip vrrp
```

**ip vrrp (vr-id)**

**Command Mode**

Interface Configuration.

**Description**

Creates a virtual router with the specified VRID and address. Use the **no** form of this command to remove a virtual router.

**Syntax**

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip vrrp <code>&lt;vr-id&gt;</code> address <code>&lt;ip-address&gt;</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>To Remove:</td>
<td><code>[no] ip vrrp </code>&lt;vr-id&gt;<code>address</code>&lt;ip-address&gt;``</td>
</tr>
</tbody>
</table>

**Table 34-1. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vr-id&gt;</code></td>
<td>The ID of the virtual router. The range is 1-255.</td>
</tr>
<tr>
<td><code>&lt;ip-address&gt;</code></td>
<td>The IP address of the virtual router.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example creates a virtual router with a vr-id of 1 and address of 10.0.1.2 on an interface labeled `boston`.

```
(config-if:boston)# ip vrrp 1 address 10.0.1.2
```

**Systems**

ip vrrp (auth-key)

Command Mode

Interface Configuration.

Description

Enables or disables the virtual router simple text password authentication for the virtual router ID. Use the no form of this command to disable simple password authentication for the virtual router.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip vrrp &lt;vr-id&gt; auth-key &lt;key-string&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>[no] ip vrrp &lt;vr-id&gt; auth-key</td>
</tr>
</tbody>
</table>

Table 34-2. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vr-id&gt;</td>
<td>Virtual router ID.</td>
</tr>
<tr>
<td>&lt;key-string&gt;</td>
<td>Simple password string.</td>
</tr>
</tbody>
</table>

Sample Output

The following example enables simple text authorization and creates a password of jerry for virtual router vr-id 1 on an interface labeled boston.

```
(config-if:boston)#  ip vrrp 1 auth-key jerry
```

Systems

ip vrrp (override)

**Command Mode**  
Interface Configuration.

**Description**  
Enables or disables the address owner override to a virtual router. The default is disabled.

**Syntax**

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip vrrp &lt;vr-id&gt; override addr owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip vrrp &lt;vr-id&gt; override addr owner</td>
</tr>
</tbody>
</table>

**Table 34-3. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vr-id&gt;</td>
<td>Virtual router ID.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example enables address owner override on virtual router vr id 1 on an interface labeled boston.

```
(config-if:boston)# ip vrrp 1 override address owner
```

**Systems**

ip vrrp (preempt)

Command Mode  Interface Configuration.

Description  Enables or disables preempt mode for a virtual router. The default is Enabled.

Syntax

<table>
<thead>
<tr>
<th>To Enable:</th>
<th>ip vrrp &lt;vr-id&gt; preempt</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Disable:</td>
<td>no ip vrrp &lt;vr-id&gt; preempt</td>
</tr>
</tbody>
</table>

Table 34-4. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vr-id&gt;</td>
<td>Virtual router ID.</td>
</tr>
</tbody>
</table>

Sample Output

The following example enables preempt mode to virtual router vr id 1 on an interface labeled boston.

(config-if:boston)# ip vrrp 1 preempt

Systems

**ip vrrp (priority)**

**Command Mode** Interface Configuration.

**Description** Sets the virtual router priority value for the virtual router ID. Use the **no** form of this command to restore the default value of 100.

**Syntax**

<table>
<thead>
<tr>
<th>Command</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>To Configure:</strong></td>
<td><code>ip vrrp &lt;vr-id&gt; priority &lt;priority-value&gt;</code></td>
</tr>
<tr>
<td><strong>To Restore Default:</strong></td>
<td><code>[no] ip vrrp &lt;vr-id&gt; priority</code></td>
</tr>
</tbody>
</table>

**Table 34-5. Parameters, Keywords, Arguments**

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;vr-id&gt;</code></td>
<td>Virtual router ID.</td>
</tr>
<tr>
<td><code>&lt;priority-value&gt;</code></td>
<td>The priority value. The range is 1 - 254. 100 is the default value.</td>
</tr>
</tbody>
</table>

**Sample Output**

The following example sets the priority value for virtual router 1 to 254 on an interface labeled *boston*.

```
(config-if:boston)# ip vrrp 1 priority 254
```

ip vrrp (timer)

Command Mode  Interface Configuration.

Description  Set the advertisement timer value for the virtual router ID. Use the no form of this command to restore the default value of 1.

Syntax

<table>
<thead>
<tr>
<th>To Configure:</th>
<th>ip vrrp &lt;vr-id&gt; timer &lt;timer-value&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Restore Default:</td>
<td>[no] ip vrrp &lt;vr-id&gt; timer</td>
</tr>
</tbody>
</table>

Sample Output  The following example sets the ip vrrp timer to 4 for virtual router 1 on an interface labeled boston.

(config-if:boston)# ip vrrp 1 timer 4


Table 34-6. Parameters, Keywords, Arguments

<table>
<thead>
<tr>
<th>Name</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vr-id&gt;</td>
<td>Virtual router ID.</td>
</tr>
<tr>
<td>&lt;timer-value&gt;</td>
<td>The advertisement transmit time. The range is 1 - 255. The default value is 1.</td>
</tr>
</tbody>
</table>
show ip vrrp

Command Mode
User.

Description
Displays VRRP information if it is enabled on the switch.

Syntax
show ip vrrp [ <if-name> [ router-id <vr-id> ] ] [ detail ]

Sample Output
The following example displays vrrp information.

> show ip vrrp
Interface VRID IP Address Pri Timer State Since
-------- ---- ----------- --- ------ ------ --------
boston 1 9.0.0.10 255 1 MASTER 09:42:13

Systems
Index

A
access list commands
  access-list 20-2
  ip access-group 20-9
  ip access-list 20-11
  ip acl-logging 20-12
  ip acl-logging logging-interval 20-13
  show access-group 20-14
  show access-lists 20-15
  show acl-match-timer 20-16
  show ip access-lists 20-17
access list 20-17
display contents 20-15
accessing
  CLI 1-5
  command modes 1-2
accessing command modes 1-2
access-list 20-2
access-list-name 20-10
AFT commands
  clear aft instance invalid-learned-entries vlan 2-2
  clear aft instance learned-entries vlan 2-3
  set aft auto-sizing-threshold 2-5
  set aft entry 2-6
  set aft instance vlan (auto-increment) 2-10
  set aft instance vlan (hash-table-size) 2-11
  set aft super-agetime 2-12
  show aft config 2-13
  show aft entry 2-14
  show aft instance 2-16
  appletalk access-group 3-2
  appletalk access-list 3-3
  appletalk address 3-5
  appletalk admin-state 3-6
  appletalk cable-range 3-7
appletalk commands
  appletalk access-group 3-2
  appletalk access-list 3-3
  appletalk address 3-5
  appletalk admin-state 3-6
  appletalk cable-range 3-7
appletalk commands, (continued)
  appletalk echo 3-8
  appletalk mac-format 3-9
  appletalk routing 3-10
  appletalk static cable-range 3-11
  appletalk vlan 3-13
  appletalk zone 3-14
  clear appletalk arp 3-15
  clear appletalk route 3-16
  clear appletalk traffic 3-17
  ping appletalk 3-18
  show appletalk access-lists 3-19
  show appletalk arp 3-20
  show appletalk globals 3-21
  show appletalk interface 3-22
  show appletalk nbp 3-23
  show appletalk route 3-24
  show appletalk static cable-range 3-25
  show appletalk traffic 3-26
  show appletalk zone 3-27
  appletalk echo 3-8
  appletalk mac-format 3-9
  appletalk routing 3-10
  appletalk static cable-range 3-11
  appletalk vlan 3-13
  appletalk zone 3-14
  area 19-3
    ase-filter 19-4
    default-cost 19-5
    nssa 19-6
    range 19-7
    stub 19-8
    translate-nssa-to-external 19-9
    virtual-link 19-10
  arp
    IP command 11-4
    arp timeout 11-5
    authentication key 12-3
    authentication mode 12-4
B
basic functions
  help 1-3
Index

boot system flash 30-4
buffering commands
set buffering fabric-port (age-timer) 4-2
set buffering fabric-port (hipri-alloc) 4-3
set buffering fabric-port (hipri-service-ratio) 4-4
set buffering fabric-port (priority threshold) 4-5
set buffering port (age-timer) 4-6
set buffering port (hipri-allocation) 4-7
set buffering port (hipri-service-ratio) 4-8
set buffering port (pri-threshold) 4-9
show buffering fabric-port 4-10
show buffering port 4-11

C
Calendar commands
 calendar set 30-5
clock set 30-9
show calendar 30-60
show clock 30-61
calendar set 30-5
CGMP
 viewing statistics 10-31
CGMP snooping
 setting 10-12
CGMP snooping statistics
 clearing 10-3
Ciphers
 show ssl ciphers 27-7
clear aft instance invalid-learned-entries vlan 2-2
clear aft instance learned-entries vlan 2-3
clear appletalk arp 3-15
clear appletalk route 3-16
clear appletalk traffic 3-17
clear arp-cache 11-6
clear cgmp statistics 10-3
clear igmp-snooping statistics 10-4
clear intelligent-multicast client-port 10-5
clear intelligent-multicast router-port-vlan 10-6
clear intelligent-multicast session 10-7
clear intelligent-multicast static-client-port 10-8
clear intelligent-multicast static-session 10-9
clear ip route 11-7
clear ipx route 13-3
clear ipx service 13-4
clear lgmp client statistics 10-7, 10-10
clear port counters 21-3
clear ssh 26-2
clear tcp 11-8
clear temperatures 31-2
clear utilization high-threshold 30-6
clear utilization monitoring 30-7
clear utilization threshold-event 30-8
clearing
 CGMP snooping statistics 10-3
 LGMP client statistics 10-10
 CLI
 accessing 1-5
client
 LGMP 10-39
client port pruning interval
 setting 10-15
client ports
 displaying 10-33
clients
 viewing 10-37
Clock
 show time zone 30-70
Clock commands
 calendar set 30-5
clock set 30-9
clock summer-time recurring 30-10
clock timezone 30-11
show calendar 30-60
show clock 30-61
clock set 30-9
clock summer-time recurring 30-10
clock timezone 30-11
command line history 1-4
command mode summaries 1-1
command syntax conventions 1-4
commands 1-4
 no form 1-4
 configure
 UI command 32-3
 connect
 UI command 32-4, 32-7
console commands
 set console baud 5-2
 set console databits 5-3
 set console flowcontrol 5-4
 set console initcmd 5-5
 set console parity 5-6
 set console stopbits 5-7
 set console transfer ppp 5-8
 set console type 5-9
 show console 5-10
 copy (running-config) 30-13
 copy (startup-config) 30-14
 copy (tftp) 30-15
copy running-config 30-20
 copy running-config startup-config 30-21
 copy running-config tftp 30-22
 copy startup-config 30-23
 copy startup-config running-config 30-24
 copy tftp 30-16, 30-17, 30-18, 30-19, 30-26, 30-29
 copy tftp bootflash 30-27, 30-47
 copy tftp flash 30-28
 copy tftp running-config 30-30
 copy tftp startup-config 30-31
 cpu-redundancy console 30-32
 cpu-redundancy Hello-Interval 30-33
 cpu-redundancy mac-prefix 30-34
 creating
 management multicast router ports 10-18

D
Daylight Savings Time
 clock summer-time recurring 30-10
 Debug mode 32-16
 default metric 12-2
 default-action-deny 20-10
 default-route-mode 12-5
 delete pcmcia 30-36
 deleting
 management multicast router ports 10-18
 dir 30-37
 disabling
 client port pruning interval 10-15
 intelligent multicast router pruning 10-19
 intelligent multicasting 10-14
 LGMP client 10-25
 router pruning 10-19
 session pruning 10-21
 displaying
 access list contents 20-15
 CGMP statistics 10-31
 client ports 10-33
 global configuration 10-34
 intelligent multicasting sessions 10-36
 IP access lists, contents of 20-17
 management configured client ports 10-37
 management configured sessions 10-38
 module information 17-5
 DVMRP
 setting neighbor timeout interval 7-7

DVMRP commands 7-1
 ip dvmrp 7-2
 ip dvmrp interface type 7-4
 ip dvmrp interface-metric 7-3
 ip dvmrp min-route-flash-update 7-5
 ip dvmrp neighbor-probe-interval 7-6
 ip dvmrp neighbor-timeout 7-7
 ip dvmrp prune-message-lifetime 7-8
 ip dvmrp remote-tunnel-address 7-9
 ip dvmrp route-limit 7-10
 ip dvmrp stats-reset 7-11
 ip dvmrp timers basic 7-12
 ip multicast prune-source 7-13
 ip multicast ttl-threshold 7-14
 router dvmrp 7-15
 show ip dvmrp 7-16
 show ip dvmrp designated forwarders 7-17
 show ip dvmrp downstream dependent routers 7-18
 show ip dvmrp forwarding cache 7-19
 show ip dvmrp interface 7-20
 show ip dvmrp interface neighbors 7-21
 show ip dvmrp routes 7-22

E
enable
 UI commands 32-8
 enabling
 client port pruning interval 10-15
 intelligent multicast router pruning 10-19
 intelligent multicasting 10-14
 LGMP client 10-25
 router pruning 10-19
 session pruning 10-21
 end
 UI command 32-9
 erase 30-38
 erase legacy-configs 30-39
 erase scripts 30-40
 erase startup-config 30-41
 exit
 UI command 32-10
 exiting
 command modes 1-2

G
global configuration
 viewing 10-34
Index

H
help
  basic functions 1-3
  UI command 32-11
hostname 30-44
hunt commands
  set huntgroup 8-2, 8-5, 8-8
  set huntgroup (redistribute) 8-4
  show huntgroup 8-6, 8-7
hunt group commands
  set huntgroup (redistribute) 8-7
  set huntgroup auto-flush 8-3

I
IGMP commands
  ip igmp 9-2
  ip igmp max-groups 9-3
  ip igmp process-leaves 9-4
  ip igmp querier 9-5, 9-6
  ip igmp query-interval 9-7
  ip igmp query-max-response-time 9-8
  ip igmp query-timeout 9-9
  ip igmp robustness 9-10
  ip igmp version 9-11
  mtrace 9-12
  router igmp 9-14
  show ip igmp groups 9-15
  show ip igmp statistics 9-16, 9-17
intelligent multicast
  removing management client ports 10-8
  removing static client ports 10-8
Intelligent Multicast Client port specifier 10-5
intelligent multicast router pruning
  disabling 10-19
  enabling 10-19
intelligent multicast sessions
  viewing 10-36
intelligent multicasting
  client port pruning interval, setting 10-15
  disabling 10-14
  disabling session pruning 10-21
  enabling 10-14
  enabling session pruning 10-21
  globally removing management sessions 10-9
  management configured sessions, viewing 10-38
  removing learned client ports 10-5
  removing learned sessions 10-7
  removing management ports 10-6
  viewing client ports 10-33
  viewing global configuration 10-34
interface 11-9
  DVMRP neighbor timeout 7-7
IP
  display contents 20-17
ip 11-39
  access group 20-9
IP access lists
  display contents 20-17
  ip access-group 20-9
  ip access-list 20-11
  ip acl Logging 20-12
  ip acl Logging logging-interval 20-13
  ip address 11-10
  ip admin state 11-11
  ip bootp dhcp agent-info 11-12
  ip bootp dhcp circuit info 11-13
  ip bootp dhcp relay 11-14
  ip bootp dhcp server 11-15
IP commands
  arp 11-4
  arp timeout 11-5
  clear arp Cache 11-6
  clear ip route 11-7
  ip address 11-10
  ip admin state 11-11
  ip bootp dhcp agent-info 11-12
  ip bootp dhcp circuit info 11-13
  ip bootp dhcp relay 11-14
  ip bootp dhcp server 11-15
  ip default gateway 6-2, 6-3, 6-4, 6-5, 11-16, 11-17, 11-18, 11-19, 11-20, 11-32
  ip http port 11-21
  ip irdp 11-22
  ip mac format 11-28
  ip max arp entries 11-29
  ip max route entries 11-30
  ip multicast-routing 11-31
  ip netbios rebroadcast 11-33
  ip net mask format 11-34
  ip proxy arp 11-35
  ip proxy arp default route 11-36
  ip proxy arp limit 11-37
  ip redirects 11-38
  ip reset stats 11-39
  ip route 11-40
  ip route preference 11-42
  ip routing 11-43
  ip routing mode 11-44
  ip source route 11-46
Index

IP commands, (continued)
ip telnet inactivity-period 11-47
ip telnet port 11-48
ip vlan 11-49
ping 11-50
redistribute 11-51
show ip arp 11-54, 11-55
show ip interface 11-56
show ip irdp 11-57
show ip route 11-59
show ip traffic 11-62
show tcp configuration 11-63
show udp statistics 11-66
ip default gateway 6-2, 6-3, 6-4, 6-5, 6-16, 11-17, 11-18, 11-19, 11-20, 11-32
ip domain-lookup 6-2, 11-19
ip domain-name 6-5, 11-20
ip dvmrp 7-2
ip dvmrp interface type 7-4
ip dvmrp interface-metric 7-3
ip dvmrp min-route-flash-update 7-5
ip dvmrp neighbor-probe-interval 7-6
ip dvmrp neighbor-timeout 7-7
ip dvmrp prune-message-lifetime 7-8
ip dvmrp remote-tunnel-address 7-9
ip dvmrp route-limit 7-10
ip dvmrp stats-reset 7-11
ip dvmrp timers basic 7-12
ip http help server 30-45
ip http port 11-21
ip https 27-2
ip igmp 9-2
ip igmp max-groups 9-3
ip igmp process-leaves 9-4
ip igmp querier 9-5, 9-6
ip igmp query-interval 9-7
ip igmp query-max-response-time 9-8
ip igmp query-timeout 9-9
ip igmp robustness 9-10
ip igmp version 9-11
ip irdp 11-22
ip irdp 11-22
ip mac-format 11-28
ip max-route-entries 11-30
ip multicast prune-source 7-13
ip multicast route-cache aging 14-2
ip multicast route-cache hash-depth 14-3
ip multicast route-cache hash-mode 14-3
ip multicast route-cache max-size 10-13
ip multicast route-cache update-timeout 14-5, 14-7
ip multicast ttl-threshold 7-14
ip multicast-routing 11-31
ip netbios-rebroadcast 11-33
ip netmask-format 11-34
ip ospf
as-boundary router 19-12
authentication-key 19-13
auto-vlink-create 19-14
cost 19-15
dead-interval 19-16
ext-route-metric 19-17
hello-interval 19-18
max-paths 19-19
message-digest-key-md5 19-20
packet tracing 19-21
reset-stats 19-23
retransmit-interval 19-22, 19-24
router-id 19-25
transmit-delay 19-26
ip proxy-arp 11-35
ip proxy-arp-default-route 11-36
ip proxy-arp-limit 11-37
ip redirects 11-38
ip reset-stats 11-39
ip rip authentication key 12-3
ip rip authentication mode 12-4
ip rip default-route-mode 12-5
ip rip poison reverse 12-6
ip rip receive version 12-7
ip rip send version 12-8
ip rip send-receive-mode 12-9
ip route 11-40
ip route-preference 11-42
ip routing 11-43
ip routing mode 11-44
ip source-route 11-46
ip ssh 26-3
ip telnet inactivity-period 11-47
ip telnet port 11-48
ip unicast route-cache aging 14-8
ip unicast route-cache hash-depth 14-9
ip unicast route-cache hash-mode 14-9
ip unicast route-cache max-size 14-10
ip unicast route-cache update-timeout 14-11
ip vlan 11-49
ip vrrp
VRRP command 34-3, 34-4
Index

ip vrrp (auth-key)
   VRRP command 34-5, 34-6, 34-7
ip vrrp (priority)
   VRRP command 34-7
ip vrrp (timer)
   VRRP command 34-9
ip-max-arp-entries 11-29
IP-RIP commands
   default-metric 12-2
   ip rip authentication key 12-3
   ip rip authentication mode 12-4
   ip rip default-route-mode 12-5
   ip rip poison-reverse 12-6
   ip rip receive version 12-7
   ip rip send version 12-8
   ip rip send-receive-mode 12-9
   neighbor 12-10
   output-delay 12-11
   router rip 12-12
   show ip rip statistics 12-15
   timers basic 12-13
   triggered updates 12-14
   ipx advertise-default-route-only 13-5
IPX commands
   clear ipx route 13-3
   clear ipx service 13-4
   ipx advertise-default-route-only 13-5
   ipx default-route 13-6
   ipx delay 13-7
   ipx down 13-8
   ipx gns-reply-disable 13-9, 13-10
   ipx network 13-11
   ipx output-rip-delay 13-13
   ipx output-sap-delay 13-14
   ipx rip 13-15
   ipx rip-filter 13-16
   ipx rip-max-packetsize 13-18
   ipx rip-multiplier 13-19
   ipx route 13-20
   ipx route-cache aging 14-12
   ipx route-cache hash-mode 14-13
   ipx route-cache max-size 14-14
   ipx route-cache update-timeout 14-15
   ipx router 13-21
   ipx routing 13-22
   ipx sap 13-23
   ipx sap-max-packetsize 13-24
   ipx sap-multiplier 13-25
   ipx sap-name-filter 13-26
   ipx sap-network-filter 13-28
   ipx send-receive-mode 13-30
   ipx send-triggered-updates 13-31
   ipx service 13-32

IPX commands, (continued)
   ipx type-20-propagation 13-34
   ipx update interval 13-35
   ipx vlan 13-36
   show ipx cache 13-37
   show ipx interface 13-38
   show ipx rip statistics 13-39
   show ipx rip-filter 13-40
   show ipx route 13-41
   show ipx sap statistics 13-42
   show ipx sap-name-filter 13-43
   show ipx sap-network-filter 13-44
   show ipx services 13-45
   show ipx traffic 13-46
   ipx default-route 13-6
   ipx delay 13-7
   ipx down 13-8
   ipx gns-reply-disable 13-9, 13-10
   ipx network 13-11
   ipx output-rip-delay 13-13
   ipx output-sap-delay 13-14
   ipx rip 13-15
   ipx rip-filter 13-16
   ipx rip-max-packetsize 13-18
   ipx rip-multiplier 13-19
   ipx route 13-20
   ipx route-cache aging 14-12
   ipx route-cache hash-mode 14-13
   ipx route-cache max-size 14-14
   ipx route-cache update-timeout 14-15
   ipx router 13-21
   ipx routing 13-22
   ipx sap 13-23
   ipx sap-max-packetsize 13-24
   ipx sap-multiplier 13-25
   ipx sap-name-filter 13-26
   ipx sap-network-filter 13-28
   ipx send-receive-mode 13-30
   ipx send-triggered-updates 13-31
   ipx service 13-32
   ipx type-20-propagation 13-31
   ipx update interval 13-35
   ipx vlan 13-36

L
   L3 Cache commands
      ip multicast route-cache aging 14-2
      ip multicast route-cache hash-mode 14-3
      ip multicast route-cache max-size 10-13
      ip multicast route-cache update-timeout 14-5, 14-7
Index

L3 Cache commands, (continued)
ip unicast route-cache aging 14-8
ip unicast route-cache hash-depth 14-9
ip unicast route-cache hash-mode 14-9
ip unicast route-cache max-size 14-10
ip unicast route-cache update-timeout 14-11
ipx route-cache aging 14-12
ipx route-cache hash-mode 14-13
ipx route-cache max-size 14-14
ipx route-cache update-timeout 14-15
show ip multicast cache 14-16
show ip unicast cache 14-17, 14-18
L3 cache commands
ip multicast route-cache hash-depth 14-3
L3 MCAST commands
clear igmp-snooping statistics 10-4
clear lgmp client statistics 10-7
set igmp-snooping 10-13
set lgmp server 10-15
set lgmp server priority 10-27
set lgmp server proxy 10-28
set lgmp server robust-variable 10-30
set lgmp server router-report-time 10-29
show igmp-snooping statistics 10-32
show lgmp server 10-40
LDAP commands
ldap search-base 15-3, 24-2
ldap server secondary 15-5, 24-4
ldap server-primary 15-4, 24-3
show ldap 6-6, 15-6, 24-5, 24-6
ldap search-base 15-3, 24-2
ldap server secondary 15-5, 24-4
ldap server-primary 15-4, 24-3
learned client ports
  removing from intelligent multicasting 10-5
learned session
  removing from intelligent multicasting 10-7
length
UI command 32-12
LGMP
  viewing client statistics 10-39
  viewing server configuration 10-39
LGMP client
  disabling 10-25
  enabling 10-25
LGMP client statistics
  clearing 10-10
  logging clear 16-2
Logging commands
  logging clear 16-2
  logging console 16-3
  logging history 16-6
  logging history size 16-9
  logging protocol event 16-10
  logging shutdown size 16-12
  logging traps 16-13
  show alarms 16-21
  show logging 16-22
  logging console 16-3
  logging history 16-6
  logging history size 16-9
  logging protocol event 16-10
  logging shutdown size 16-12
  logging traps 16-13
M
management client ports
  removing from intelligent multicast 10-8
management configured client ports
displaying 10-37
management configured sessions
  viewing 10-38
management multicast router ports
  creating 10-18
  deleting 10-18
management ports
  removing from intelligent multicasting 10-6
management sessions
  globally removing from intelligent multicasting 10-9
MCAST commands
  clear cgmp statistics 10-3
  clear intelligent-multicast client-port 10-5
  clear intelligent-multicast router-port-vlan
  10-6
  clear intelligent-multicast session 10-7
  clear intelligent-multicast static-client-port
  10-8
  clear intelligent-multicast static-session 10-9
  clear lgmp client statistics 10-10
  set cgmp 10-12
  set intelligent-multicast 10-14
  set intelligent-multicast client-port-pruning
  10-16
  set intelligent-multicast client-port-pruning
  time 10-17
  set intelligent-multicast router-port vlan 10-31
MCAST commands, (continued)
  set intelligent-multicast router-port-pruning 10-18
  set intelligent-multicast router-port-pruning time 10-20
  set intelligent-multicast session-pruning 10-21
  set intelligent-multicast session-pruning time 10-22
  set intelligent-multicast static-client-port 10-23
  set intelligent-multicast static-session 10-24
  set igmp client 10-25
  show cgmp statistics 10-31
  show intelligent-multicast client-port 10-33
  show intelligent-multicast configuration 10-34
  show intelligent-multicast router-port 10-35
  show intelligent-multicast session 10-36
  show intelligent-multicast static-client 10-37
  show intelligent-multicast static-session 10-38
  show igmp client 10-39
  mod-name 17-3
  mod-notes 17-4
  mod-num 17-3
  module
    displaying information 17-5
    notes, setting 17-4
    setting name 17-3
  module commands
    set module name 17-3
    set module notes 17-4
    show module 17-5
  module name
    setting 17-3
  mtrace 9-12, 9-13
  multicast router
    creating on specific VLANs 10-18
  multicast router port
    removing from configuration 10-19
  multicast session
    dynamically learned 10-7
    removing from configuration 10-21
    statically created 10-7

N
  name
    module, setting 17-3
  neighbor
    IP-RIP command 32-5
  network
    IP-RIP command 12-10
    network area 19-27, 19-28
  no form 1-4
  no network area 19-27, 19-28
  notes
    setting module 17-4
    notes page 17-4
  nvram initialize 30-46

O
  OSPF commands
    area 19-3
    area as-filter 19-4
    area default-cost 19-5
    area nssa 19-6
    area range 19-7
    area stub 19-8
    area translate-nssa-to-external 19-9
    area virtual-link 19-10
    interface 11-9
    ip ospf as-boundary router 19-12
    ip ospf authentication-key 19-13
    ip ospf auto-vlink-create 19-14
    ip ospf cost 19-15
    ip ospf dead-interval 19-16
    ip ospf ext-route-meteric 19-17
    ip ospf hello-interval 19-18
    ip ospf max-paths 19-19
    ip ospf message-digest-key md5 19-20
    ip ospf packet tracing 19-21
    ip ospf reset-stats 19-23
    ip ospf retransmit-interval 19-22, 19-24
    ip ospf router-id 19-25
    ip ospf transmit-delay 19-26
    network area 19-27, 19-28
    router ospf 19-29
    show ip ospf 19-30
    show ip ospf database 19-31
    show ip ospf interface 19-32
    show ip ospf neighbor 19-33, 19-34
    show ip ospf virtual-links 19-35
    timers lsa-group-pacing 19-36
    timers spf 19-37
  output delay
  IP-RIP command 12-11

P
  password 32-13
  ping
    IP command 11-50
    ping appletalk 3-18
    poison reverse 12-6
Index

Policy commands
   ip access-list 20-11
   show access-group 20-14
   show access-lists 20-15
   show ip access-lists 20-17
Port commands 21-1
   {set | clear} port huntgroup 21-6
   clear port counters 21-3
   set port 3com-mapping-table 21-4
   set port allow-learning 21-5
   set port auto-negotiation 21-7
   set port auto-negotiation-duplex-advertisement 21-8
   set port auto-negotiation-speed-advertisement 21-10, 21-11
   set port auto-vlan-create 21-11
   set port category 21-12
   set port disable 21-13
   set port duplex 21-14
   set port enable 21-16
   set port mirror 21-24
   set port speed 21-41
   set port trunking-format 21-42
   set port vlan 21-43
   set port vlan-binding-method 21-44
   set port vtp-snooping 21-45
   show port 21-46
   show port counters 21-47
   show port mirror 21-48
   show port status 21-51
Power Cool RAM commands
   show system fans 22-2
   show system power 22-3
   show system ram 22-4

R
Rapid Spanning Tree commands
   set port edge admin state 21-15, 28-2
   set port point-to-point admin status 21-33,
     28-3
   set port spanning-tree-mode 28-4
   set port spantree force-protocol-migration 28-5
   set port spantree priority 28-7
   set spantree 28-9
   set spantree config 28-11
   set spantree default-path-cost 28-12
   set spantree fwddelay 28-14
   set spantree hello 28-16
   set spantree hold-count 28-17
   set spantree maxage 28-18
   set spantree portcost 28-20
   Rapid Spanning Tree commands, (continued)
     set spantree priority 28-23
     set spantree version 28-25
     show spantree 28-26
     show spantree blocked 28-28
     show spantree config 28-29
     show spantree port 28-30
     show spantree version 28-32
     receive version 12-7
     redistribute 11-51
     reload 30-48
     removing
       multicast router ports 10-19
       multicast sessions 10-21
     reset 30-49
     router dvmrp 7-15
     router igmp 9-14
     router ospf 19-29
     router pruning
       disabling 10-19
       enabling 10-19
     router rip
       IP-RIP command 12-12
     router vrrp 34-2
     router-DVMRP
       ip dvmrp min-route-flash-update 7-5
S
   search criteria
     for viewing intelligent multicast sessions 10-36
 Secure Mode
   secure-mode 30-50
   show secure-mode 30-67
   secure-mode 30-50
   send version 12-8
   send-receive-mode 12-9
   serial interface
     using 1-5
   server
     LGMP 10-39
   server configuration
     LGMP 10-39
   session pruning
     disabling 10-21
     enabling 10-21
   session-id 10-33
   set 3com-mapping-table 33-2
   set aft auto-sizing-threshold 2-5
   set aft entry 2-6
   set aft instance vlan (auto-increment) 2-10
set aft instance vlan (hash-table-size) 2-11
set aft super-agetime 2-12
set buffering fabric-port (age-timer) 4-2
set buffering fabric-port (hipri-alloc) 4-3
set buffering fabric-port (hipri-service-ratio) 4-4
set buffering fabric-port (priority threshold) 4-5
set buffering port (age-timer) 4-6
set buffering port (hipri-alloc) 4-7
set buffering port (hipri-service-ratio) 4-8
set buffering port (priority threshold) 4-9
set console baud 5-2
set console databits 5-3
set console flowcontrol 5-4
set console initcmd 5-5
set console parity 5-6
set console stopbits 5-7
set console transfer ppp 5-8
set console type 5-9
set debug 32-16
set fabric configure-redundant-hardware 29-2
set fabric enable-redundant-element 29-3
set fabric toggle-active-controller 29-4
set huntgroup 8-2, 8-5, 8-8
set huntgroup (redistribute) 8-4, 8-7
set huntgroup auto-flush 8-3
set igmp-snooping 10-13
set intelligent-multicast 10-14
set intelligent-multicast client-port-pruning 10-15, 10-16
set intelligent-multicast client-port-pruning time 10-17
set intelligent-multicast router-port vlan 10-18
set intelligent-multicast router-port-pruning 10-19
set intelligent-multicast router-port-pruning time 10-20
set intelligent-multicast session-pruning 10-21
set intelligent-multicast session-pruning time 10-22
set intelligent-multicast static-client-port 10-23
set intelligent-multicast static-session 10-24
set igmp client 10-25
set igmp server 10-15, 10-26
set igmp server priority 10-27
set igmp server proxy 10-28
set igmp server robust-variable 10-30
set igmp server router-report-time 10-29
set login 32-17
set module name 17-3
set module notes 17-4
set port 3com-mapping-table 21-4
set port allow-learning 21-5
set port auto-negotiation 21-7
set port auto-negotiation-duplex-advertisement 21-8
set port auto-negotiation-speed-advertisement 21-10, 21-11
set port auto-vlan-create 21-11
set port category 21-12
set port disable 21-13
set port duplex 21-14
set port edge admin state 21-15, 28-2
set port enable 21-16
set port mirror 21-24
set port point-to-point admin status 21-33, 28-3
set port spanning-tree-mode 28-4
set port spantree force-protocol-migration 28-5
set port spantree priority 28-7
set port speed 21-41
set port truning-format 21-42
set port vlan 21-43
set port vlan-binding-method 21-44
set port vtp-snooping 21-45
set spantree 28-9
set spantree config 28-11
set spantree default-path-cost 28-12
set spantree fwddelay 28-14
set spantree hello 28-16
set spantree hold-count 28-17
set spantree maxage 28-18
set spantree portcost 28-20
set spantree priority 28-23
set spantree version 28-25
set temperature (shutdown) 31-3
set temperature (warning) 31-4
set utilization high-threshold 30-54
set utilization monitoring 30-56
set utilization threshold-event 30-57
set vlan
detailed 33-9
set vlan (frame format) 33-4
set vlan ID 33-3
set vtp-snooping 33-5
set vtp-snooping domain 33-7
setting
CGMP snooping 10-12
DVMRP neighbor timeout interval 7-7
module name 17-3
module notes 17-4
setup 30-58
show 3com-mapping-table 33-8
show access-group 20-14
show access-lists 20-15
show acl-match-timer 20-16
show aft config 2-13
show aft entry 2-14
show aft instance 2-16
show alarms
  Logging command 16-21
show appletalk access-lists 3-19
show appletalk arp 3-20
show appletalk globals 3-21
show appletalk interface 3-22
show appletalk nbp 3-23
show appletalk route 3-24
show appletalk static cable-range 3-25
show appletalk traffic 3-26
show appletalk zone 3-27
show arp 11-53
show boot 30-59, 30-62, 30-63
show buffering fabric-port 4-10
show buffering port 4-11
show calendar 30-60
show cgmp statistics 10-31
show clock 30-61
show console 5-10
show fabric status 29-5
show file_name 30-64
show flash 30-65
show history 32-19
  UI command 32-14, 32-19
show huntgroup 8-6, 8-7
show igmp-snooping statistics 10-32
show intelligent-multicast client-port 10-33
show intelligent-multicast configuration 10-34
show intelligent-multicast router-port 10-35
show intelligent-multicast session 10-36
show intelligent-multicast static-client 10-37
show intelligent-multicast static-session 10-38
show ip access-lists 20-17
show ip arp 11-54, 11-55
show ip dvmrp 7-16
show ip dvmrp designated forwarders 7-17
show ip dvmrp downstream dependent routers 7-18
show ip dvmrp forwarding cache 7-19
show ip dvmrp interface 7-20
show ip dvmrp interface neighbors 7-21
show ip dvmrp routes 7-22
show ip igmp groups 9-15
show ip igmp statistics 9-16, 9-17
show ip interface 11-56
show ip irdp
  ip irdp 11-57
show ip multicast cache 14-16
show ip ospf 19-30
  interface 19-32
  neighbor 19-33, 19-34
  virtual-links 19-35
show ip ospf database 19-31
show ip rip statistics 12-15
show ip route 18-2, 18-4, 18-5, 21-30
  ip route 11-59
show ip traffic
  ip traffic 11-62
show ip unicast cache 14-17, 14-18
show ip vrrp
  VRRP command 34-10
show ipx cache 13-37
show ipx interface 13-38
show ipx rip statistics 13-39
show ipx rip-filter 13-40
show ipx route 13-41
show ipx sap statistics 13-42
show ipx sap-name-filter 13-43
show ipx sap-network-filter 13-44
show ipx services 13-45
show ipx traffic 13-46
show ldap 6-6, 15-6, 24-5, 24-6
show lgmp client 10-39
show lgmp server 10-40
show logging 16-22
show login 32-20
show module 17-5
show port 21-46
show port counters 21-47
show port mirror 21-48
show port status 21-51
show running-config 30-66
show secure-mode 30-67
show sessions
  UI command 32-21
show snntp 30-68
show spanning-tree 28-26
show spanning-tree blocked 28-28
show spanning-tree config 28-29
show spanning-tree port 28-30
show spanning-tree version 28-32
show ssh 26-7
show ssl cert 27-3
show ssl certreq 27-5
show ssl ciphers 27-7
show ssl config 27-7, 27-8
show startup-config 30-69
show system fans 22-2
show system power 22-3
show system ram 22-4
show tcp configuration 11-63
show temperature 31-6
show time zone 30-70
show udp statistics 11-66
show username 32-22
show utilization results 30-71
show utilization settings 30-72
show version 30-73
show vtp-snooping configuration 33-10
SNMP commands
  hostname 30-44
  ip igmp query-max-response-time 9-8
snooping
  CGMP 10-12
snooping statistics
  clearing CGMP 10-3
SNTP
  show sntp 30-68
Spanning Tree commands
  set port edge admin state 21-15, 28-2
  set port point-to-point admin status 21-33, 28-3
  set port spanning-tree-mode 28-4
  set port spantree force-protocol-migration 28-5
  set port spantree priority 28-7
  set spantree 28-9
  set spantree config 28-11
  set spantree default-path-cost 28-12
  set spantree fddelay 28-14
  set spantree hello 28-16
  set spantree hold-count 28-17
  set spantree maxage 28-18
  set spantree portcost 28-20
  set spantree priority 28-23
  set spantree version 28-25
  show spantree 28-26
  show spantree blocked 28-28
  show spantree config 28-29
  show spantree port 28-30
  show spantree version 28-32
  ssh 26-4
  SSL commands
    clear ssh 26-2
    ip ssh 26-3
    show ssh 26-7
    ssh 26-4
    ssh keygen 26-5
    ssh timeout 26-6
    ssh keygen 26-5
    ssh timeout 26-6
    ssl backcert 27-9
    ssl certreq 27-10
    ssl restart 27-11
    ssl selfcert 27-12
  SSL/HTTPS commands
    ip https 27-2
    show ssl cert 27-3
    show ssl certreq 27-5
    show ssl ciphers 27-7
    show ssl config 27-7, 27-8
    ssl backcert 27-9
    ssl certreq 27-10
    ssl restart 27-11
    ssl selfcert 27-12
static client ports
  removing from intelligent multicast 10-8
static session 10-37
statistics
  LGMP client 10-10
  udp 11-66
  viewing CGMP 10-31
  viewing LGMP 10-39
Switch Fab commands
  set fabric configure-redundant-hardware 29-2
  set fabric enable-redundant-element 29-3
  set fabric toggle-active-controller 29-4
  show fabric status 29-5
Switch IP commands
  show arp 11-53
  show ip route 18-2
System commands 30-1
  boot system flash 30-4
  copy (running-config) 30-13
  copy (startup-config) 30-14
  copy (tftp) 30-15
  copy running-config 30-20
  copy running-config startup-config 30-21
  copy running-config tftp 30-22
  copy startup-config 30-23
System commands, (continued)
copy startup-config running-config 30-24
copy startup-config tftp 30-25
copy tftp 30-16, 30-17, 30-18, 30-19, 30-26, 30-29
copy tftp bootflash 30-27, 30-47
copy tftp flash 30-28
copy tftp running-config 30-30
copy tftp startup-config 30-31
dir 30-37
erase 30-38
erase legacy-configs 30-39
erase scripts 30-40
erase startup-config 30-41
ip http help server 30-45
nvram initialize 30-46
reload 30-48
reset 30-49
setup 30-58
show boot 30-59, 30-62, 30-63
show file_name 30-64
show flash 30-65
show running-config 30-66
show startup-config 30-69
show version 30-73

timers
lsa-group-pacing 19-36
spf 19-37
timers basic
IP-RIP command 12-13
triggered update
IP-RIP command 12-14

U
udp statistics 11-66
UI commands
configure 32-3
connect 32-4, 32-7
enable 32-8
end 32-9
exit 32-10
help 32-11
length 32-12
show history 32-14, 32-19
show sessions 32-21
telnet 32-23
terminal databits 32-24
terminal flowcontrol 32-25
terminal length 32-26
terminal output pause 32-27
terminal parity 32-28
terminal speed 32-29
terminal stopbits 32-30
terminal width 32-31
width 32-34

User accounts
Create 32-32
Disable 32-32
Expiration 32-32
password 32-13
set login 32-17
show login 32-20
show username 32-22
username 32-32
using telnet 1-5
using the serial interface 1-5
utilization monitoring commands
clear utilization high-threshold 30-6
clear utilization monitoring 30-7
clear utilization threshold-event 30-8
set utilization high-threshold 30-54
set utilization monitoring 30-56
set utilization threshold-event 30-57
show utilization results 30-71
show utilization settings 30-72

T
TCP
clear TCP 11-8
tcp connections 11-63
telnet
UI commands 32-23
using 1-5
Temperatures commands
clear temperatures 31-2
set temperature (shutdown) 31-3
set temperature (warning) 31-4
show temperature 31-6
terminal databits
UI command 32-24
terminal flowcontrol 32-25
terminal length 32-26
terminal output pause 32-27
terminal parity 32-28
terminal speed 32-29
terminal stopbits 32-30
terminal width 32-31
Time zone commands
clock timezone 30-11
Time zones
show time zone 30-70
Index

V
viewing
  CGMP statistics 10-31
  client ports 10-33
  clients 10-37
  intelligent multicast sessions 10-36
  management configured client ports 10-37
  management configured sessions 10-38
VLAN all 10-37
VLAN commands
  set vlan 33-3
  set vlan (frame format) 33-4
  set vtp-snooping 33-5
  set vtp-snooping domain 33-7
  show vlan detailed 33-9
  show vtp-snooping configuration 33-10
vlan detailed 33-9
VLANs
  creating multicast routers on 10-18
VRRP commands
  ip vrrp 34-3, 34-4
  ip vrrp (auth-key) 34-5, 34-6, 34-7
  ip vrrp (priority) 34-7
  ip vrrp (timer) 34-9
  router vrrp 34-2
  show ip vrrp 34-10
vtp-snooping 33-5
vtp-snooping domain 33-7

W
width
  UI command 32-34