HP Procurve
Series 5300XL Switches

Software Release E.08.xx or Greater

Advanced Traffic Management Guide
Publication Number
5990-6051
February 2004
Edition 1

Applicable Products
- HP ProCurve Switch 5308XL (J4819A)
- HP ProCurve Switch 5372XL (J4848A)
- HP ProCurve Switch 5348XL (J4849A)
- HP ProCurve Switch 5304XL (J4850A)

Trademark Credits
Microsoft, Windows, Windows 95, and Microsoft Windows NT are US registered trademarks of Microsoft Corporation. Internet Explorer is a trademark of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Netscape is a registered trademark of Netscape Corporation. Cisco® is a trademark of Cisco Systems, Inc.

Disclaimer
The information contained in this document is subject to change without notice.

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

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

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

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

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

1 Getting Started

Contents .......................................................... 1-1
Overview ......................................................... 1-2
Conventions ...................................................... 1-2
  Command Syntax Statements ............................... 1-2
  Command Prompts ............................................. 1-3
  Screen Simulations ........................................... 1-3
Related Publications ........................................... 1-3
Getting Documentation From the Web ..................... 1-5
Sources for More Information ................................ 1-6
Need Only a Quick Start? ...................................... 1-7
  IP Addressing .................................................. 1-7
  To Set Up and Install the Switch in Your Network ..... 1-7

2 Static Virtual LANs (VLANs)

Contents .......................................................... 2-1
Overview .......................................................... 2-2
Introduction ...................................................... 2-3
  General VLAN Operation ..................................... 2-3
  Types of VLANs Available in the Switch ................. 2-4
    Port-Based VLANs .......................................... 2-4
    Protocol-Based VLANs .................................... 2-4
    Designated VLANs ......................................... 2-4
Terminology ...................................................... 2-5
Static VLAN Operation ......................................... 2-6
  VLAN Environments ......................................... 2-7
  VLAN Operation ................................................ 2-8
    The Default VLAN .......................................... 2-8
Multiple Port-Based VLANs ........................................ 2-8
Protocol VLAN Environment .................................. 2-9
Routing Options for VLANs .................................. 2-9
Overlapping (Tagged) VLANs ................................. 2-9

VLAN Operating Rules .......................................... 2-13

General Steps for Using VLANs .............................. 2-16

Multiple VLAN Considerations ............................... 2-17
  Single Forwarding Database Operation .................. 2-18
  Multiple Forwarding Database Operation .............. 2-20

Configuring VLANs ............................................. 2-21
  Menu: Configuring Port-Based VLAN Parameters .... 2-21
    To Change VLAN Support Settings .................. 2-21
    Adding or Editing VLAN Names .................... 2-24
    Adding or Changing a VLAN Port Assignment ...... 2-25
  CLI: Configuring Port-Based and Protocol-Based VLAN
  Parameters .................................................. 2-27
  Web: Viewing and Configuring VLAN Parameters ...... 2-37

802.1Q VLAN Tagging ........................................ 2-38

Special VLAN Types .......................................... 2-43
  VLAN Support and the Default VLAN .................. 2-43
  The Primary VLAN ........................................ 2-43
  The Secure Management VLAN ............................ 2-44
    Preparation ............................................. 2-46
    Configuration ......................................... 2-47
    Deleting the Management VLAN ........................ 2-48
    Operating Notes for Management VLANs .......... 2-48
  Voice VLANs ............................................... 2-49
    Operating Rules for Voice VLANs .................... 2-49
    Components of Voice VLAN Operation ............... 2-50
    Voice VLAN QoS Prioritizing (Optional) .......... 2-50
    Voice VLAN Access Security ......................... 2-51
Effect of VLANs on Other Switch Features ............................ 2-51
Spanning Tree Operation with VLANs ................................. 2-51
IP Interfaces ................................................................. 2-52
VLAN MAC Address ....................................................... 2-52
Port Trunks ................................................................. 2-52
Port Monitoring ............................................................ 2-52
VLAN Restrictions ......................................................... 2-53

3 GVRP

Contents ................................................................. 3-1
Overview ................................................................. 3-2
Introduction ............................................................. 3-3
General Operation ...................................................... 3-4
Per-Port Options for Handling GVRP “Unknown VLANs” ........ 3-7
Per-Port Options for Dynamic VLAN Advertising and Joining . 3-9
GVRP and VLAN Access Control ........................................ 3-11
Planning for GVRP Operation .......................................... 3-12
Configuring GVRP On a Switch ......................................... 3-13
  Menu: Viewing and Configuring GVRP ............................. 3-13
  CLI: Viewing and Configuring GVRP ............................... 3-14
  Web: Viewing and Configuring GVRP ............................... 3-18
GVRP Operating Notes .................................................. 3-18

4 Multimedia Traffic Control with IP Multicast (IGMP)

Contents ................................................................. 4-1
Overview ................................................................. 4-2
IGMP General Operation and Features .............................. 4-3
  IGMP Terms .......................................................... 4-4
  IGMP Operating Features ........................................... 4-5
    Basic Operation .................................................. 4-5
    Enhancements ..................................................... 4-5
  CLI: Configuring and Displaying IGMP ........................... 4-6
Web: Enabling or Disabling IGMP ........................................ 4-11

How IGMP Operates ...................................................... 4-11
  Operation With or Without IP Addressing ...................... 4-13
  Automatic Fast-Leave IGMP .................................. 4-13
  Forced Fast-Leave IGMP ..................................... 4-15
    Configuration Options for Forced Fast-Leave ............ 4-15
    Listing the Forced Fast-Leave Configuration .......... 4-16
    Configuring Per-Port Forced Fast-Leave IGMP .......... 4-18

Using the Switch as Querier ........................................ 4-19

Excluding Well-Known or Reserved Multicast Addresses
from IP Multicast Filtering ..................................... 4-20
  IP Multicast Filters ....................................... 4-21
  Reserved Addresses Excluded from IP Multicast (IGMP)
    Filtering .................................................. 4-21
  Number of IP Multicast Addresses Allowed .............. 4-21

5 PIM-DM (Dense Mode)

Contents ............................................................. 5-1
Overview ............................................................ 5-2
Introduction ......................................................... 5-3
Feature Overview ................................................... 5-4
PIM-DM Operation .................................................... 5-4
  Multicast Flow Management ................................ 5-7
  General Configuration Elements ......................... 5-9
Terminology .......................................................... 5-9
PIM-DM Operating Rules ............................................ 5-10
Configuring PIM-DM .................................................. 5-11
  PIM Global Configuration Context ...................... 5-12
  PIM VLAN (Interface) Configuration Context .......... 5-15
Displaying PIM Data and Configuration Settings .......... 5-22
  Displaying PIM Route Data ................................ 5-23
  Displaying PIM Status .................................... 5-27
Operating Notes ..................................................... 5-34
6 Spanning-Tree Operation

Contents .................................................................................................................. 6-1
Overview ................................................................................................................... 6-2
The RSTP (802.1w) and STP (802.1D) Spanning Tree Options ..................... 6-5
   RSTP (802.1w) .................................................................................................... 6-6
   STP (802.1D) ..................................................................................................... 6-6
   How STP and RSTP Operate ............................................................................ 6-7
Configuring Rapid Reconfiguration Spanning Tree (RSTP) ......................... 6-9
   Overview ............................................................................................................. 6-9
   Transitioning from STP to RSTP ..................................................................... 6-10
   Configuring RSTP ............................................................................................. 6-11
      Optimizing the RSTP Configuration ............................................................. 6-11
      CLI: Configuring RSTP .................................................................................. 6-12
      Menu: Configuring RSTP ............................................................................. 6-18
      Web: Enabling or Disabling RSTP .............................................................. 6-20
802.1D Spanning-Tree Protocol (STP) ............................................................... 6-21
   Menu: Configuring 802.1D STP .................................................................... 6-21
   CLI: Configuring 802.1D STP ......................................................................... 6-24
   STP Fast Mode .................................................................................................. 6-28
   Fast-Uplink Spanning Tree Protocol (STP) ..................................................... 6-29
      Terminology ................................................................................................... 6-31
      Operating Rules for Fast Uplink .................................................................. 6-32
      Menu: Viewing and Configuring Fast-Uplink STP ....................................... 6-33
      CLI: Viewing and Configuring Fast-Uplink STP ........................................ 6-39
      Operating Notes ............................................................................................. 6-42
Web: Enabling or Disabling STP ......................................................................... 6-43
802.1s Multiple Spanning Tree Protocol (MSTP) ..................... 6-44
   MSTP Structure .................................................. 6-45
   How MSTP Operates .............................................. 6-47
   MST Regions ....................................................... 6-47
   Regions, Legacy STP and RSTP Switches, and the Common
   Spanning Tree (CST) ................................................ 6-49
   MSTP Operation with 802.1Q VLANs .............................. 6-49
Terminology .......................................................... 6-50
Operating Rules ...................................................... 6-52
Transitioning from STP or RSTP to MSTP ............................ 6-53
Tips for Planning an MSTP Application .............................. 6-54
Steps for Configuring MSTP ......................................... 6-55
Configuring MSTP Operation Mode and Global Parameters ...... 6-57
Configuring Basic Port Connectivity Parameters ................. 6-61
Configuring MST Instance Parameters ............................. 6-63
Configuring MST Instance Per-Port Parameters .................... 6-66
Enabling or Disabling Spanning Tree Operation .................... 6-69
Enabling an Entire MST Region at Once or Exchanging One
Region Configuration for Another .................................. 6-69
Displaying MSTP Statistics and Configuration .................... 6-71
   Displaying MSTP Statistics ........................................ 6-71
   Displaying the MSTP Configuration ................................ 6-74
Operating Notes ...................................................... 6-78
Troubleshooting ...................................................... 6-78

7 Switch Meshing

Contents ............................................................. 7-1
Introduction ......................................................... 7-2
Switch Meshing Fundamentals ...................................... 7-4
   Terminology ........................................................ 7-4
   Operating Rules .................................................... 7-5
   Using a Heterogeneous Switch Mesh ................................ 7-7
   Bringing Up a Switch Mesh Domain: ............................. 7-10
Further Operating Information ...................................... 7-10
8 Quality of Service (QoS): Managing Bandwidth More Effectively

Contents .................................................................................. 8-1

Introduction .............................................................................. 8-2
   Terminology ........................................................................... 8-5
   Overview ............................................................................... 8-6

Classifiers for Prioritizing Outbound Packets ...................... 8-8

Preparation for Configuring QoS ............................................. 8-11

Using QoS Classifiers To Configure Quality of Service for
Outbound Traffic ................................................................. 8-13
   QoS UDP/TCP Priority ......................................................... 8-13
      Assigning a Priority Based on TCP or UDP Port Number .... 8-14
      Assigning a DSCP Policy Based on TCP or UDP Port
      Number ........................................................................... 8-15
   QoS IP-Device Priority ......................................................... 8-19
      Assigning a Priority Based on IP Address ......................... 8-19
      Assigning a DSCP Policy Based on IP Address ............... 8-20
QoS IP Type-of-Service (ToS) Policy and Priority .......................... 8-24
Assigning an 802.1p Priority to IP Packets on the Basis of the ToS Precedence Bits ......................................................... 8-25
Assigning an 802.1p Priority to IP Packets on the Basis of Incoming DSCP ................................................................. 8-26
Assigning a DSCP Policy on the Basis of the DSCP in IP Packets Received from Upstream Devices ....................... 8-30
Details of QoS IP Type-of-Service ........................................ 8-33
QoS LAN Protocol Priority .................................................... 8-36
QoS VLAN-ID (VID) Priority .................................................. 8-38
Assigning a Priority Based on VLAN-ID Only ......................... 8-38
Assigning a DSCP Policy Based on VLAN-ID (VID) .............. 8-40
QoS Source-Port Priority ....................................................... 8-43
Assigning a Priority Based on Source-Port Only ...................... 8-44
Assigning a DSCP Policy Based on the Source-Port ............... 8-46
Differentiated Services Codepoint (DSCP) Mapping ............... 8-50
Default Priority Settings for Selected Codepoints ................. 8-51
Quickly Listing Non-Default Codepoint Settings ...................... 8-51
Note On Changing a Priority Setting ..................................... 8-53

Configuring QoS from the Web Browser Interface .................. 8-56
IP Multicast (IGMP) Interaction with QoS ............................... 8-57
QoS Messages in the CLI ...................................................... 8-57
QoS Operating Notes ........................................................... 8-58

9 Access Control Lists (ACLs)

Contents .............................................................................. 9-1
Introduction ......................................................................... 9-3
Terminology .......................................................................... 9-5
Overview .............................................................................. 9-8
Types of IP ACLs .................................................................. 9-8
ACL Inbound and Outbound Application Points .................... 9-8
Features Common to All ACLs ............................................. 9-9
General Steps for Planning and Configuring ACLs ................. 9-10
ACL Operation ................................................................. 9-12
  Introduction ............................................................... 9-12
  The Packet-Filtering Process ........................................ 9-13

Planning an ACL Application ........................................... 9-16
  Traffic Management and Improved Network Performance .......... 9-16
  Security ................................................................. 9-17
  Guidelines for Planning the Structure of an ACL .................. 9-18
  ACL Configuration and Operating Rules .............................. 9-18
  How an ACE Uses a Mask To Screen Packets for Matches ......... 9-20
    What Is the Difference Between Network (or Subnet) Masks
    and the Masks Used with ACLs? .................................. 9-20
    Rules for Defining a Match Between a Packet and an
    Access Control Entry (ACE) ........................................ 9-21

Configuring and Assigning an ACL .................................... 9-25
  Overview ............................................................... 9-25
    General Steps for Implementing ACLs ............................... 9-25
    Types of ACLs ...................................................... 9-26
  ACL Configuration Structure .......................................... 9-26
    Standard ACL Structure ............................................ 9-27
    Extended ACL Configuration Structure ............................. 9-28
  ACL Configuration Factors ............................................ 9-29
    The Sequence of Entries in an ACL Is Significant .............. 9-29
    In Any ACL, There Will Always Be a Match ....................... 9-31
    A Configured ACL Has No Effect Until You Apply It to an
    Interface ............................................................ 9-31
  Using the CLI To Create an ACL ..................................... 9-31
    General ACE Rules .................................................. 9-32
    Using CIDR Notation To Enter the ACL Mask ....................... 9-32
  Configuring and Assigning a Numbered, Standard ACL ............. 9-33
  Configuring and Assigning a Numbered, Extended ACL ............ 9-38
  Configuring a Named ACL ............................................. 9-44
  Enabling or Disabling ACL Filtering on a VLAN .................... 9-46

Deleting an ACL from the Switch ...................................... 9-47
Displaying ACL Data ................................................................. 9-48
  Display an ACL Summary ...................................................... 9-48
  Display the Content of All ACLs on the Switch ....................... 9-49
  Display the ACL Assignments for a VLAN ............................... 9-50
  Displaying the Content of a Specific ACL ............................... 9-51
  Display All ACLs and Their Assignments in the Switch Startup-Config File and Running-Config File ......................... 9-53

Editing ACLs and Creating an ACL Offline .................................. 9-53
  Using the CLI To Edit ACLs .................................................. 9-53
    General Editing Rules .................................................... 9-54
    Deleting Any ACE from an ACL .......................................... 9-54
    Working Offline To Create or Edit an ACL ............................. 9-56

Enable ACL “Deny” Logging ...................................................... 9-59
  Requirements for Using ACL Logging ...................................... 9-59
  ACL Logging Operation ..................................................... 9-60
  Enabling ACL Logging on the Switch ...................................... 9-60
  Operating Notes for ACL Logging ........................................... 9-62

General ACL Operating Notes .................................................. 9-63

10  IP Routing Features

  Contents .............................................................................. 10-1

  Overview of IP Routing ...................................................... 10-3
    IP Interfaces ..................................................................... 10-4
    IP Tables and Caches ...................................................... 10-4
      ARP Cache Table .......................................................... 10-5
      IP Route Table ............................................................ 10-5
      IP Forwarding Cache .................................................... 10-6
    IP Route Exchange Protocols ............................................. 10-7
    IP Global Parameters for Routing Switches ......................... 10-7
    IP Interface Parameters for Routing Switches ...................... 10-9

  Configuring IP Parameters for Routing Switches ...................... 10-10
    Configuring IP Addresses .................................................. 10-10
    Changing the Router ID .................................................... 10-10
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring ARP Parameters</td>
<td>10-11</td>
</tr>
<tr>
<td>How ARP Works</td>
<td>10-11</td>
</tr>
<tr>
<td>Enabling Proxy ARP</td>
<td>10-13</td>
</tr>
<tr>
<td>Configuring Forwarding Parameters</td>
<td>10-13</td>
</tr>
<tr>
<td>Changing the TTL Threshold</td>
<td>10-14</td>
</tr>
<tr>
<td>Enabling Forwarding of Directed Broadcasts</td>
<td>10-14</td>
</tr>
<tr>
<td>Configuring ICMP</td>
<td>10-15</td>
</tr>
<tr>
<td>Disabling ICMP Messages</td>
<td>10-15</td>
</tr>
<tr>
<td>Disabling Replies to Broadcast Ping Requests</td>
<td>10-15</td>
</tr>
<tr>
<td>Disabling ICMP Destination Unreachable Messages</td>
<td>10-16</td>
</tr>
<tr>
<td>Disabling ICMP Redirects</td>
<td>10-17</td>
</tr>
<tr>
<td>Configuring Static IP Routes</td>
<td>10-17</td>
</tr>
<tr>
<td>Static Route Types</td>
<td>10-17</td>
</tr>
<tr>
<td>Static IP Route Parameters</td>
<td>10-18</td>
</tr>
<tr>
<td>Static Route States Follow Port States</td>
<td>10-18</td>
</tr>
<tr>
<td>Configuring a Static IP Route</td>
<td>10-19</td>
</tr>
<tr>
<td>Configuring a “Null” Route</td>
<td>10-19</td>
</tr>
<tr>
<td>Configuring RIP</td>
<td>10-21</td>
</tr>
<tr>
<td>Overview of RIP</td>
<td>10-21</td>
</tr>
<tr>
<td>RIP Parameters and Defaults</td>
<td>10-22</td>
</tr>
<tr>
<td>RIP Global Parameters</td>
<td>10-22</td>
</tr>
<tr>
<td>RIP Interface Parameters</td>
<td>10-22</td>
</tr>
<tr>
<td>Configuring RIP Parameters</td>
<td>10-23</td>
</tr>
<tr>
<td>Enabling RIP</td>
<td>10-23</td>
</tr>
<tr>
<td>Changing the RIP Type on a VLAN Interface</td>
<td>10-24</td>
</tr>
<tr>
<td>Changing the Cost of Routes Learned on a VLAN Interface</td>
<td>10-24</td>
</tr>
<tr>
<td>Configuring RIP Redistribution</td>
<td>10-25</td>
</tr>
<tr>
<td>Define RIP Redistribution Filters</td>
<td>10-25</td>
</tr>
<tr>
<td>Modify Default Metric for Redistribution</td>
<td>10-26</td>
</tr>
<tr>
<td>Enable RIP Route Redistribution</td>
<td>10-26</td>
</tr>
<tr>
<td>Changing the Route Loop Prevention Method</td>
<td>10-27</td>
</tr>
<tr>
<td>Displaying RIP Information</td>
<td>10-27</td>
</tr>
<tr>
<td>Displaying General RIP Information</td>
<td>10-28</td>
</tr>
<tr>
<td>Displaying RIP Interface Information</td>
<td>10-30</td>
</tr>
<tr>
<td>Displaying RIP Peer Information</td>
<td>10-31</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Displaying RIP Redistribution Information</td>
<td>10-33</td>
</tr>
<tr>
<td>Displaying RIP Redistribution Filter (restrict) Information</td>
<td>10-33</td>
</tr>
<tr>
<td><strong>Configuring OSPF</strong></td>
<td>10-34</td>
</tr>
<tr>
<td>Overview of OSPF</td>
<td>10-34</td>
</tr>
<tr>
<td>Designated Routers in Multi-Access Networks</td>
<td>10-35</td>
</tr>
<tr>
<td>Designated Router Election</td>
<td>10-35</td>
</tr>
<tr>
<td>OSPF RFC 1583 and 2328 Compliance</td>
<td>10-36</td>
</tr>
<tr>
<td>Reduction of Equivalent AS External LSAs</td>
<td>10-36</td>
</tr>
<tr>
<td>Dynamic OSPF Activation and Configuration</td>
<td>10-38</td>
</tr>
<tr>
<td><strong>Configuring OSPF</strong></td>
<td>10-38</td>
</tr>
<tr>
<td>Configuration Rules</td>
<td>10-39</td>
</tr>
<tr>
<td>OSPF Parameters</td>
<td>10-39</td>
</tr>
<tr>
<td>Enabling OSPF on the Series 5300XL Switch</td>
<td>10-40</td>
</tr>
<tr>
<td>Assigning OSPF Areas</td>
<td>10-40</td>
</tr>
<tr>
<td>Assigning an Area Range (optional)</td>
<td>10-42</td>
</tr>
<tr>
<td>Assigning VLANs to an Area</td>
<td>10-43</td>
</tr>
<tr>
<td>Modifying Interface Defaults</td>
<td>10-43</td>
</tr>
<tr>
<td>OSPF Interface Parameters</td>
<td>10-44</td>
</tr>
<tr>
<td>Assigning Virtual Links</td>
<td>10-45</td>
</tr>
<tr>
<td>Modifying Virtual Link Parameters</td>
<td>10-47</td>
</tr>
<tr>
<td>Virtual Link Parameter Descriptions</td>
<td>10-47</td>
</tr>
<tr>
<td>Defining Redistribution Filters</td>
<td>10-48</td>
</tr>
<tr>
<td>Modifying Default Metric for Redistribution</td>
<td>10-49</td>
</tr>
<tr>
<td>Enabling Route Redistribution</td>
<td>10-50</td>
</tr>
<tr>
<td>Modifying Redistribution Metric Type</td>
<td>10-50</td>
</tr>
<tr>
<td>Administrative Distance</td>
<td>10-50</td>
</tr>
<tr>
<td>Modifying OSPF Traps Generated</td>
<td>10-51</td>
</tr>
<tr>
<td>Modifying OSPF Standard Compliance Setting</td>
<td>10-52</td>
</tr>
<tr>
<td><strong>Displaying OSPF Information</strong></td>
<td>10-53</td>
</tr>
<tr>
<td>Displaying General OSPF Configuration Information</td>
<td>10-53</td>
</tr>
<tr>
<td>Displaying OSPF Area Information</td>
<td>10-55</td>
</tr>
<tr>
<td>Displaying OSPF External Link State Information</td>
<td>10-56</td>
</tr>
<tr>
<td>Displaying OSPF Interface Information</td>
<td>10-57</td>
</tr>
<tr>
<td>Displaying OSPF Interface Information for a Specific VLAN or IP Address</td>
<td>10-58</td>
</tr>
</tbody>
</table>
Displaying OSPF Link State Information ................. 10-60
Displaying OSPF Neighbor Information ................. 10-62
Displaying OSPF Redistribution Information .......... 10-64
Displaying OSPF Redistribution Filter (restrict) Information 10-64
Displaying OSPF Virtual Neighbor Information ....... 10-65
Displaying OSPF Virtual Link Information .......... 10-66
Displaying OSPF Route Information .................. 10-68

Configuring IRDP ........................................ 10-70
  Enabling IRDP Globally ................................ 10-71
  Enabling IRDP on an Individual VLAN Interface ... 10-71
  Displaying IRDP Information ....................... 10-72

Configuring DHCP Relay ................................ 10-73
  Overview ............................................. 10-73
  DHCP Packet Forwarding ............................. 10-73
    Unicast Forwarding ................................. 10-73
    Broadcast Forwarding .............................. 10-73
  Minimum Requirements for DHCP Relay Operation ... 10-74
  Enabling DHCP Relay ................................ 10-74
  Configuring a Helper Address ...................... 10-74
  Viewing the Current DHCP Relay Configuration .... 10-75

Configuring Static Network Address Translation (NAT) for Intranet Applications ........................................ 10-76
  Static NAT Operating Rules ......................... 10-77
  Configuring Static NAT ............................... 10-77
  Displaying Static NAT Statistics and Configuration 10-79
  Static NAT Operating Notes ....................... 10-79

11 Router Redundancy Using XRRP

Contents .................................................. 11-1
Introduction to XRRP .................................... 11-2
Terminology ............................................. 11-2
Overview of XRRP Operation ........................................ 11-3
  XRRP During Normal Router Operation ....................... 11-4
  XRRP Fail-Over Operation .................................... 11-5
    Single VLAN Operation .................................... 11-5
    Multiple VLAN Operation ................................. 11-6
  XRRP Operation Notes ........................................ 11-9

Configuring XRRP .................................................. 11-11
  Customizing the XRRP Configuration ....................... 11-12
  Enabling and Disabling XRRP .............................. 11-15
  Configuration Rules ......................................... 11-15
  Configuration Examples .................................... 11-16
    Configuration for Figure 11-2 – Single VLAN Example .... 11-16
    Configuration for Figure 11-4 – Multiple VLANs ......... 11-17

Displaying XRRP Data .............................................. 11-18

Comparison Between XRRP and VRRP ........................... 11-21

Index
Getting Started

Contents

Overview ................................................................. 1-2
Conventions ............................................................... 1-2
   Command Syntax Statements .................................. 1-2
   Command Prompts ............................................... 1-3
   Screen Simulations .............................................. 1-3
Related Publications .................................................. 1-3
Getting Documentation From the Web ........................ 1-5
Sources for More Information ................................. 1-6
Need Only a Quick Start? ........................................... 1-7
   IP Addressing ...................................................... 1-7
   To Set Up and Install the Switch in Your Network .... 1-7
Overview

This *Advanced Traffic Guide* is intended for use with the following switches:

- HP Procurve Switch 5304XL
- HP Procurve Switch 5348XL
- HP Procurve Switch 5308XL
- HP Procurve Switch 5372XL

Together, these four devices are termed the *Series 5300XL switches*.

This guide describes how to use the command line interface (CLI), Menu interface, and web browser interface to configure, manage, monitor, and troubleshoot switch operation. The *Product Documentation CD-ROM* shipped with the switch includes a copy of this guide. You can also download a copy from the HP Procurve website. (See “Getting Documentation From the Web” on page 1-5.)

For information on other product documentation for Series 5300XL switch, refer to “Related Publications” on page 1-3.

Conventions

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

Command Syntax Statements

**Syntax:** `aaa port-access authenticator < port-list >`

- Vertical bars (`|`) separate alternative, mutually exclusive elements.
- Square brackets (`[ ]`) indicate optional elements.
- Braces (`<>`) enclose required elements.
- Braces within square brackets (`[<>]`) indicate a required element within an optional choice.
- Boldface indicates use of a CLI command, part of a CLI command syntax, or other displayed element in general text. For example:

  “Use the `copy tftp` command to download the key from a TFTP server.”

- Italics indicate variables for which you must supply a value when executing the command. For example, in this command syntax, you must provide one or more port numbers:

  **Syntax:** `aaa port-access authenticator < port-list >`
Command Prompts

In the default configuration, your Series 5300XL switch displays one of the following CLI prompts:

   HP Procurve Switch 5304#
   HP Procurve Switch 5308#

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

   HPswitch#

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

Screen Simulations

Figures containing simulated screen text and command output look like this:

```
HPswitch> show version
Image stamp: /sw/code/build/info
            June 1 2004 13:43:13
            E.08.01
            139
HPswitch>
```

Figure 1-1. Example of a Figure Showing a Simulated Screen

In some cases, brief command-output sequences appear without figure identification. For example:

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

Related Publications

Software Release Notes. Release notes are posted on the HP Procurve website and provide information on new software updates:

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

To view and download a copy of the latest release notes for your switch, see “Getting Documentation From the Web” on page 1-5.
Product Notes. The printed Read Me First shipped with your switch provides product notes, and other information. For the latest version, refer to “Getting Documentation From the Web” on page 1-5.

Installation and Getting Started Guide. Use the Installation and Getting Started Guide shipped with your switch to prepare for and perform the physical installation. This guide also steps you through connecting the switch to your network and assigning IP addressing, as well as describing the LED indications for correct operation and trouble analysis. A PDF version of this guide is also provided on the Product Documentation CD-ROM shipped with the switch. And you can download a copy from the HP Procurve website. (See “Getting Documentation From the Web” on page 1-5.)

Management and Configuration Guide. Use the Management and Configuration Guide for information on:
- Using the command line, Menu, and web browser interfaces
- Learning how memory operates in the switch
- IP addressing
- Time protocols
- Port configuration options
- Interaction with network management applications
- Transfers of various file types related to switch operation
- Monitoring and troubleshooting switch software operation
- MAC addressing
- Daylight time rules

Access Security Guide. Use the Access Security Guide to learn how to use and configure the following access security features available in the switch:
- Username and Password Security
- Web Authentication and MAC Authentication
- TACACS+ Authentication
- RADIUS authentication and Accounting
- Secure Shell (SSH) Encryption
- Port-Based Access Control (802.1x)
- Port Security Using Authorized MAC Addresses
- MAC Lockout and MAC Lockdown
- Authorized IP Managers
- Key Management System

HP provides PDF versions of the switch documentation on the Product Documentation CD-ROM shipped with the switch. You can also download the latest version of any HP ProCurve switch manual (in PDF format) from the HP ProCurve website. (See “Getting Documentation From the Web” on page 1-5.)
Getting Documentation From the Web

1. Go to the HP Procurve website at http://www.hp.com/go/hpprocurve
2. Click on technical support.
3. Click on manuals.
4. Click on the product for which you want to view or download a manual.

Figure 1-2. Example of How To Locate Product Manuals on the HP ProCurve Website
Sources for More Information

- If you need information on specific parameters in the menu interface, refer to the online help provided in the interface. For example:

![Figure 1-3.Example of How To Display Online Help for the Menu Interface](image)

- If you need information on a specific command in the CLI, type the command name followed by “help”. For example:

```
HPswitch# write help
Usage: write <memory|terminal>

Description: View or save the running configuration of the switch.

write terminal - displays the running configuration of the switch on the terminal
write memory - saves the running configuration of the switch to flash. The saved configuration becomes the boot-up configuration of the switch the next time it is booted.
```

![Figure 1-4.Example of How To Display Help for a CLI Command](image)

- If you need information on specific features in the HP Web Browser Interface (hereafter referred to as the “web browser interface”), use the online help available for the web browser interface. For more information on web browser Help, refer to “Online Help for the HP Web Browser Interface” in the chapter titled “Using the HP Web Browser Interface” in the Management and Configuration Guide for your switch.
If you need further information on Hewlett-Packard switch technology, visit the HP Procurve website at:

http://www.hp.com/go/hpprocurve

Need Only a Quick Start?

IP Addressing

If you just want to give the switch an IP address so that it can communicate on your network, or if you are not using VLANs, HP recommends that you use the Switch Setup screen to quickly configure IP addressing. To do so, do one of the following:

- Enter `setup` at the CLI Manager level prompt.
  
  HPswitch# setup

- In the Main Menu of the Menu interface, select

  8. Run Setup

For more on using the Switch Setup screen, see the *Installation and Getting Started Guide* you received with the switch.

To Set Up and Install the Switch in Your Network

Use the *HP Procurve Series 5300 Installation and Getting Started Guide* (shipped with the switch) for the following:

- Notes, cautions, and warnings related to installing and using the switch and its related modules

- Instructions for physically installing the switch in your network

- Quickly assigning an IP address and subnet mask, set a Manager password, and (optionally) configure other basic features.

- Interpreting LED behavior.
— This page is intentionally unused. —
# Static Virtual LANs (VLANs)

## Contents

**Overview** ................................................................. 2-2

**Introduction** ............................................................. 2-3
  - General VLAN Operation .............................................. 2-3
  - Types of Static VLANs Available in the Switch ................ 2-4
    - Port-Based VLANs .................................................. 2-4
    - Protocol-Based VLANs .......................................... 2-4
    - Designated VLANs ................................................ 2-4

**Terminology** ............................................................ 2-5

**Static VLAN Operation** ................................................ 2-6
  - VLAN Environments .................................................. 2-7
  - VLAN Operation ...................................................... 2-8
    - The Default VLAN ................................................ 2-8
    - Multiple Port-Based VLANs ...................................... 2-8
    - Protocol VLAN Environment ..................................... 2-9
    - Routing Options for VLANs ..................................... 2-9
    - Overlapping (Tagged) VLANs ................................... 2-9

**VLAN Operating Rules** ................................................ 2-13

**General Steps for Using VLANs** ..................................... 2-16

**Multiple VLAN Considerations** ...................................... 2-17

**Configuring VLANs** .................................................... 2-21
  - Menu: Configuring Port-Based VLAN Parameters ................. 2-21
  - CLI: Configuring Port-Based and Protocol-Based VLAN Parameters ....................................................... 2-27
  - Web: Viewing and Configuring VLAN Parameters ............... 2-37
Overview

This chapter describes how to configure and use static, port-based and protocol-based VLANs on the Series 5300XL switches.

For general information on how to use the switch’s built-in interfaces, refer to these chapters in the Management and Configuration Guide for your switch:

- Chapter 3, “Using the Menu Interface”
- Chapter 4, “Using the Command Line Interface (CLI)”
- Chapter 5, “Using the HP Web Browser Interface”
- Chapter 6, “Switch Memory and Configuration”
Introduction

VLAN Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view existing VLANs</td>
<td>n/a</td>
<td>page 2-21 thru 2-27</td>
<td>page 2-28</td>
<td>page 2-37</td>
</tr>
<tr>
<td>configuring static VLANs</td>
<td>default VLAN with VID = 1</td>
<td>page 2-21 thru 2-27</td>
<td>page 2-27</td>
<td>page 2-37</td>
</tr>
</tbody>
</table>

VLANs enable you to group users by logical function instead of physical location. This helps to control bandwidth usage within your network by allowing you to group high-bandwidth users on low-traffic segments and to organize users from different LAN segments according to their need for common resources and/or their use of individual protocols. You can also improve traffic control at the edge of your network by separating traffic of different protocol types. VLANs can also enhance your network security by creating separate subnets to help control in-band access to specific network resources.

General VLAN Operation

A VLAN is comprised of multiple ports operating as members of the same subnet (broadcast domain). Ports on multiple devices can belong to the same VLAN, and traffic moving between ports in the same VLAN is bridged (or "switched"). (Traffic moving between different VLANs must be routed.) A static VLAN is an 802.1Q-compliant VLAN configured with one or more ports that remain members regardless of traffic usage. (A dynamic VLAN is an 802.1Q-compliant VLAN membership that the switch temporarily creates on a port to provide a link to another port in the same VLAN on another device.)

This chapter describes static VLANs configured for port-based or protocol-based operation. Static VLANs are configured with a name, VLAN ID number (VID), and port members. (For dynamic VLANs, refer to chapter 3, “GVRP”.)

By default, the Switch 5300XL Series devices are 802.1Q VLAN-enabled and allow up to 256 static and dynamic VLANs. (The default static VLAN setting is 8). 802.1Q compatibility enables you to assign each switch port to multiple VLANs, if needed.
Types of Static VLANs Available in the Switch

Port-Based VLANs

This type of static VLAN creates a specific layer-2 broadcast domain comprised of member ports that bridge IPv4 traffic among themselves. Port-Based VLAN traffic is routable on Switch Series 5300XL devices.

Protocol-Based VLANs

This type of static VLAN creates a layer-3 broadcast domain for traffic of a particular protocol, and is comprised of member ports that bridge traffic of the specified protocol type among themselves. Some protocol types are routable on the Switch Series 5300XL. Refer to table 2-1 on page 2-6.

Designated VLANs

The switch uses these static, port-based VLAN types to separate switch management traffic from other network traffic. While these VLANs are not limited to management traffic only, they can provide improved security and availability for management traffic.

- **The Default VLAN:** This port-based VLAN is always present in the switch and, in the default configuration, includes all ports as members (page 2-43).

- **The Primary VLAN:** The switch uses this port-based VLAN to run certain features and management functions, including DHCP/Bootp responses for switch management. In the default configuration, the Default VLAN is also the Primary VLAN. However, you can designate another, port-based, non-default VLAN, as the Primary VLAN (page 2-43).

- **The Secure Management VLAN:** This optional, port-based VLAN establishes an isolated network for managing the HP ProCurve switches that support this feature. Access to this VLAN and to the switch’s management functions are available only through ports configured as members (page 2-44).

- **Voice VLANs:** This optional, port-based VLAN type enables you to separate, prioritize, and authenticate voice traffic moving through your network, and to avoid the possibility of broadcast storms affecting VoIP (Voice-over-IP) operation (page 2-49).
In a multiple-VLAN environment that includes some older switch models there may be problems related to the same MAC address appearing on different ports and VLANs on the same switch. In such cases the solution is to impose some cabling and VLAN restrictions. For more on this topic, refer to “Multiple VLAN Considerations” on page 2-17.

**Terminology**

**Dynamic VLAN:** An 802.1Q VLAN membership temporarily created on a port linked to another device, where both devices are running GVRP. (See also Static VLAN.) For more information, refer to chapter 3, “GVRP”.

**Static VLAN:** A port-based or protocol-based VLAN configured in switch memory. (See also Dynamic VLAN.)

**Tagged Packet:** A packet that carries an IEEE 802.1Q VLAN ID (VID), which is a two-byte extension that precedes the source MAC address field of an ethernet frame. A VLAN tag is layer 2 data and is transparent to higher layers.

**Tagged VLAN:** A VLAN that complies with the 802.1Q standard, including priority settings, and allows a port to join multiple VLANs. (See also Untagged VLAN.)

**Untagged Packet:** A packet that does not carry an IEEE 802.1Q VLAN ID (VID).

**Untagged VLAN:** A VLAN that does not use or forward 802.1Q VLAN tagging, including priority settings. A port can be a member of only one untagged VLAN of a given type (port-based and the various protocol-based types). (See also Tagged VLAN.)

**VID:** The acronym for a VLAN Identification Number. Each
Static VLAN Operation

A group of networked ports assigned to a VLAN form a broadcast domain that is separate from other VLANs that may be configured on the switch. On a given switch, packets are bridged between source and destination ports that belong to the same VLAN. Thus, all ports passing traffic for a particular subnet address should be configured to the same VLAN. Cross-domain broadcast traffic in the switch is eliminated and bandwidth is saved by not allowing packets to flood out all ports.

Table 2-1. Comparative Operation of Port-Based and Protocol-Based VLANs

<table>
<thead>
<tr>
<th>Port-Based VLANs</th>
<th>Protocol-Based VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Addressing</strong></td>
<td>Usually configured with at least one unique IP address. You can create a port-based VLAN without an IP address. However, this limits the switch features available to ports on that VLAN. (Refer to “How IP Addressing Affects Switch Operation” in the chapter on configuring IP addressing in the Basic Management and Configuration Guide for the switch.) You can also use multiple IP addresses to create multiple subnets within the same VLAN. (For more on this topic, refer to the chapter on configuring IP addressing in the Basic Management and Configuration Guide for the switch.)</td>
</tr>
<tr>
<td><strong>Untagged VLAN Membership</strong></td>
<td>A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.</td>
</tr>
</tbody>
</table>
### Static Virtual LANs (VLANs)

#### Static VLAN Operation

<table>
<thead>
<tr>
<th>Port-Based VLANs</th>
<th>Protocol-Based VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tagged VLAN Membership</strong></td>
<td>A port can be a tagged member of any port-based VLAN. See above.</td>
</tr>
</tbody>
</table>
| **Routing** | The switch can internally route IP (IPv4) traffic between port-based VLANs and between port-based and IPv4 protocol-based VLANs if the switch configuration enables IP routing. If the switch is not configured to route traffic internally between port-based VLANs, then an external router must be used to move traffic between VLANs. | If the switch configuration enables IP routing, the switch can internally route IPv4 traffic as follows:  
- Between multiple IPv4 protocol-based VLANs  
- Between IPv4 protocol-based VLANs and port-based VLANs. Other protocol-based VLANs require an external router for moving traffic between VLANs. |

**Note:** NETbeui, SNA, and DEClat are non-routable protocols. End stations intended to receive traffic in these protocols must be attached to the same physical network.

#### Commands for Configuring Static VLANs

- **Tagged VLAN Membership**

  ```
  vlan <VID> [ tagged | untagged < [e] port-list >]
  ```

- **Protocol-Based VLANs**

  ```
  vlan <VID> [ tagged | untagged < [e] port-list >]
  ```

### VLAN Environments

You can configure different VLAN types in any combination. Note that the default VLAN will always be present. (For more on the default VLAN, refer to “VLAN Support and the Default VLAN” on page 2-43.)

#### Table 2-2. VLAN Environments

<table>
<thead>
<tr>
<th>VLAN Environment</th>
<th>Elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The default VLAN (port-based; VID of “1”) Only</strong></td>
<td>In the default VLAN configuration, all ports belong to VLAN 1 as untagged members. VLAN 1 is a port-based VLAN, for IPv4 traffic.</td>
</tr>
<tr>
<td><strong>Multiple VLAN Environment</strong></td>
<td>In addition to the default VLAN, the configuration can include one or more other port-based VLANs and one or more protocol VLANs. (The switch allows up to 256 VLANs of all types.) Using VLAN tagging, ports can belong to multiple VLANs of all types. Enabling routing on the switch enables the switch to route IPv4 traffic between port-based VLANs and between port-based VLANs and IPv4 protocol VLANs. Routing other types of traffic between VLANs requires an external router capable of processing the appropriate protocol(s).</td>
</tr>
</tbody>
</table>
VLAN Operation

The Default VLAN. In figure 2-1, all ports belong to the default VLAN, and devices connected to these ports are in the same broadcast domain. Except for an IP address and subnet, no configuration steps are needed.

Multiple Port-Based VLANs. In figure 2-2, routing within the switch is disabled (the default). This means that communication between any routable VLANs on the switch must go through the external router. In this case, VLANs “W” and “X” can exchange traffic through the external router, but traffic in VLANs “Y” and “Z” is restricted to the respective VLANs. Note that VLAN 1, the default VLAN, is also present, but not shown. (The default VLAN cannot be deleted from the switch. However, ports assigned to other VLANs can be removed from the default VLAN, if desired.) If internal (IP) routing is enabled on the switch, then the external router is not needed for traffic to move between port-based VLANs.
**Protocol VLAN Environment.** Figure 2-2 can also be applied to a protocol VLAN environment. In this case, VLANs “W” and “X” represent routable protocol VLANs. VLANs “Y” and “Z” can be any protocol VLAN. As noted for the discussion of multiple port-based VLANs, VLAN 1 is not shown. Enabling internal (IP) routing on the switch allows IP traffic to move between VLANs on the switch. However, routable, non-IP traffic always requires an external router.

**Routing Options for VLANs**

**Table 2-3. Options for Routing Between VLAN Types in the Switch**

<table>
<thead>
<tr>
<th>Port-Based Protocol</th>
<th>IPX</th>
<th>IPv4</th>
<th>IPv6</th>
<th>ARP</th>
<th>AppleTalk</th>
<th>SNA&lt;sup&gt;2&lt;/sup&gt;</th>
<th>DEClat&lt;sup&gt;2&lt;/sup&gt;</th>
<th>Netbeui&lt;sup&gt;2&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-Based IPX</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Port-Based IPv4</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Port-Based IPv6</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Yes&lt;sup&gt;1&lt;/sup&gt;</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Port-Based ARP</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Yes&lt;sup&gt;1&lt;/sup&gt;</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Port-Based AppleTalk</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Port-Based SNA&lt;sup&gt;2&lt;/sup&gt;</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Yes&lt;sup&gt;1&lt;/sup&gt;</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Port-Based DEClat&lt;sup&gt;2&lt;/sup&gt;</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Port-Based Netbeui&lt;sup&gt;2&lt;/sup&gt;</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

<sup>1</sup>Requires an external router to route between VLANs.

<sup>2</sup>Not a routable protocol type. End stations intended to receive traffic in these protocols must be attached to the same physical network.

**Overlapping (Tagged) VLANs**

A port can be a member of more than one VLAN of the same type if the device to which the port connects complies with the 802.1Q VLAN standard. For example, a port connected to a central server using a network interface card (NIC) that complies with the 802.1Q standard can be a member of multiple VLANs, allowing members of multiple VLANs to use the server. Although these VLANs cannot communicate with each other through the server, they can all access the server over the same connection from the switch. Where VLANs
overlap in this way, VLAN “tags” are used in the individual packets to distin-
guish between traffic from different VLANs. A VLAN tag includes the particu-
lar VLAN I.D. (VID) of the VLAN on which the packet was generated.

Figure 2-3. Example of Overlapping VLANs Using the Same Server

Similarly, using 802.1Q-compliant switches, you can connect multiple VLANs
through a single switch-to-switch link.

Figure 2-4. Example of Connecting Multiple VLANs Through the Same Link

**Introducing Tagged VLAN Technology into Networks Running Legacy (Untagged) VLANs.** You can introduce 802.1Q-compliant devices into net-
works that have built untagged VLANs based on earlier VLAN technology. The
fundamental rule is that legacy/untagged VLANs require a separate link for
each VLAN, while 802.1Q, or tagged VLANs can combine several VLANs in one
link. This means that on the 802.1Q-compliant device, separate ports (config-
ured as untagged) must be used to connect separate VLANs to non-802.1Q
devices.
Static Virtual LANs (VLANs)

Red VLAN

Blue VLAN

Red VLAN

Blue VLAN

Red Server

ProCurve Switch

Blue Server

ProCurve Switch

Non-802.1Q Switch

The legacy (non-802.1Q compliant) switch requires a separate link for each VLAN.

VLAN tagging enables the Link to carry Red VLAN and Blue VLAN Traffic

Figure 2-5. Example of Tagged and Untagged VLAN Technology in the Same Network

For more information on VLANs, refer to:

■ “Overview of Using VLANs” (page 2-43)
■ “Menu: Configuring VLAN Parameters (page 2-21)
■ “CLI: Configuring VLAN Parameters” (page 2-21)
■ “Web: Viewing and Configuring VLAN Parameters” (page 2-37)
■ “VLAN Tagging Information” (page 2-38)
■ “Effect of VLANs on Other Switch Features” (page 2-51)
■ “VLAN Restrictions” (page 2-53)

Per-Port Static VLAN Configuration Options

The following figure and table show the options you can use to assign individual ports to a static VLAN. Note that GVRP, if configured, affects these options and VLAN behavior on the switch. The display below shows the per-port VLAN configuration options. Table 2-4 briefly describes these options.
### Example of Per-Port VLAN Configuration with GVRP Disabled (the default)

<table>
<thead>
<tr>
<th>Port</th>
<th>DEFAULT_VLAN</th>
<th>VLAN-22</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Untagged</td>
<td>Forbid</td>
</tr>
<tr>
<td>A2</td>
<td>No</td>
<td>Tagged</td>
</tr>
<tr>
<td>A3</td>
<td>No</td>
<td>Tagged</td>
</tr>
<tr>
<td>A4</td>
<td>Forbid</td>
<td>Tagged</td>
</tr>
<tr>
<td>A5</td>
<td>Untagged</td>
<td>No</td>
</tr>
</tbody>
</table>

### Example of Per-Port VLAN Configuration with GVRP Enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>DEFAULT_VLAN</th>
<th>VLAN-22</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Untagged</td>
<td>Forbid</td>
</tr>
<tr>
<td>A2</td>
<td>Auto</td>
<td>Tagged</td>
</tr>
<tr>
<td>A3</td>
<td>Auto</td>
<td>Tagged</td>
</tr>
<tr>
<td>A4</td>
<td>Forbid</td>
<td>Tagged</td>
</tr>
<tr>
<td>A5</td>
<td>Untagged</td>
<td>Auto</td>
</tr>
</tbody>
</table>

Enabling GVRP causes “No” to display as “Auto”.

![Figure 2-6. Comparing Per-Port VLAN Options With and Without GVRP](image)

### Table 2-4. Per-Port VLAN Configuration Options

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Effect on Port Participation in Designated VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tagged</td>
<td>Allows the port to join multiple VLANs.</td>
</tr>
<tr>
<td>Untagged</td>
<td>Allows VLAN connection to a device that is configured for an untagged VLAN instead of a tagged VLAN. A port can be an untagged member of only one port-based VLAN. A port can also be an untagged member of only one protocol-based VLAN for any given protocol type. For example, if the switch is configured with the default VLAN plus three protocol-based VLANs that include IPX, then port 1 can be an untagged member of the default VLAN and one of the protocol-based VLANs.</td>
</tr>
</tbody>
</table>
| No - or - Auto | **No**: Appears when the switch is not GVRP-enabled; prevents the port from joining that VLAN.  
**Auto**: Appears when GVRP is enabled on the switch; allows the port to dynamically join any advertised VLAN that has the same VID |
| Forbid    | Prevents the port from joining the VLAN, even if GVRP is enabled on the switch. |
VLAN Operating Rules

- **DHCP/Bootp**: If you are using DHCP/Bootp to acquire the switch’s configuration, packet time-to-live, and TimeP information, you must designate the VLAN on which DHCP is configured for this purpose as the Primary VLAN. (In the factory-default configuration, the DEFAULT_VLAN is the Primary VLAN.)

- **Per-VLAN Features**: IGMP and some other features operate on a “per VLAN” basis. This means you must configure such features separately for each VLAN in which you want them to operate.

- **Default VLAN**: You can rename the default VLAN, but you cannot change its VID (1) or delete it from the switch.

- **VLAN Port Assignments**: Any ports not specifically removed from the default VLAN remain in the DEFAULT_VLAN, regardless of other port assignments. Also, a port must always be a tagged or untagged member of at least one port-based VLAN.

- **Voice-Over-IP (VoIP)**: VoIP operates only over static, port-based VLANs.

- **Multiple VLAN Types Configured on the Same Port**: A port can simultaneously belong to both port-based and protocol-based VLANs.

- **Protocol Capacity**: A protocol-based VLAN can include up to three protocol types. In protocol VLANs using the IPv4 protocol, ARP must be one of these protocol types (to support normal IP network operation). Otherwise, IP traffic on the VLAN is disabled. If you configure an IPv4 protocol VLAN that does not already include the ARP VLAN protocol, the switch displays this message:

```
HPswitch(config)# vlan 97 protocol ipv4
[Caution: IPv4 assigned without ARP, this may result in undeliverable IP packets.]
```  

- **Deleting Static VLANs**: If one or more ports are assigned to a non-default VLAN, you cannot delete that VLAN from the switch configuration until you first remove the port(s) from the VLAN configuration.

- **Adding or Deleting VLANs**: Changing the number of VLANs supported on the switch requires a reboot. (From the CLI, you must perform a `write memory` command before rebooting.) Other VLAN configuration changes are dynamic.
- **Inbound Tagged Packets**: If a tagged packet arrives on a port that is not a tagged member of the VLAN indicated by the packet’s VID, the switch drops the packet. Similarly, the switch will drop an inbound, tagged packet if the receiving port is an *untagged* member of the VLAN indicated by the packet’s VID.

- **Untagged Packet Forwarding**: To enable an inbound port to forward an untagged packet, the port must be an untagged member of either a protocol VLAN matching the packet’s protocol or an untagged member of a port-based VLAN. That is, when a port receives an incoming, untagged packet, it processes the packet according to the following ordered criteria:

  1. If the port has no untagged VLAN memberships, the switch drops the packet.

  2. If the port has an untagged VLAN membership in a protocol VLAN that matches the protocol type of the incoming packet, then the switch forwards the packet on that VLAN.

  3. If the port is a member of an untagged, port-based VLAN, the switch forwards the packet to that VLAN. Otherwise, the switch drops the packet.
**Static Virtual LANs (VLANs)**

**VLAN Operating Rules**

- Port "X" receives an inbound, untagged Packet.

- Is the port an untagged member of any VLANs?
  - No: Drop the packet.
  - Yes:
    - Does the packet's protocol match the protocol of an untagged VLAN membership on the port?
      - No: Drop the packet.
      - Yes: Forward the packet on the protocol VLAN.

- Is the port a member of an untagged, port-based VLAN?
  - No: Drop the packet.
  - Yes: Forward the packet on the port-based VLAN.

---

**Figure 2-7. Untagged VLAN Operation**

- **Tagged Packet Forwarding:** If a port is a tagged member of the same VLAN as an inbound, tagged packet received on that port, then the switch forwards the packet to an outbound port on that VLAN. (To enable the forwarding of tagged packets, any VLAN to which the port belongs as a
tagged member must have the same VID as that carried by the inbound, tagged packets generated on that VLAN.)

Figure 2-8. Tagged VLAN Operation

See also “Multiple VLAN Considerations” on page 2-17.

General Steps for Using VLANs

1. Plan your VLAN strategy and create a map of the logical topology that will result from configuring VLANs. Include consideration for the interaction between VLANs and other features such as Spanning Tree Protocol, port trunking, and IGMP. (Refer to “Effect of VLANs on Other Switch Features” on page 2-51.) If you plan on using dynamic VLANs, include the port configuration planning necessary to support this feature. (Refer to chapter 3, “GVRP”.)

By default, VLAN support is enabled and the switch is configured for eight VLANs.

2. Configure at least one VLAN in addition to the default VLAN.

3. Assign the desired switch ports to the new VLAN(s).
4. If you are managing VLANs with SNMP in an IP network, the VLAN through which you are managing the switch must have an IP address. Refer to chapter 7, “Configuring IP Addressing”, in the *Management and Configuration Guide* for your switch.

## Multiple VLAN Considerations

Switches use a *forwarding database* to maintain awareness of which external devices are located on which VLANs. Some switches, such as the Series 5300XL family, have a *multiple forwarding database*, which means the switch allows multiple database entries of the same MAC address, with each entry showing the (different) source VLAN and source port. Other switch models have a *single forwarding database*, which means they allow only one database entry of a unique MAC address, along with the source VLAN and source port on which it is found. All VLANs on an HP ProCurve series 5300XL switch use the same MAC address. Thus, connecting a Series 5300XL (multiple forwarding database) switch to a single forwarding database switch where multiple VLANs exist imposes some cabling and port VLAN assignment restrictions. Table 2-5 illustrates the functional difference between the two database types.

**Table 2-5. Example of Forwarding Database Content**

<table>
<thead>
<tr>
<th></th>
<th>Multiple Forwarding Database</th>
<th>Single Forwarding Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Destination VLAN ID</td>
<td>Destination Port</td>
</tr>
<tr>
<td>0004ea-84d9f4</td>
<td>1</td>
<td>A5</td>
</tr>
<tr>
<td>0004ea-84d9f4</td>
<td>22</td>
<td>A12</td>
</tr>
<tr>
<td>0004ea-84d9f4</td>
<td>44</td>
<td>A20</td>
</tr>
<tr>
<td>0060b0-880a81</td>
<td>33</td>
<td>A20</td>
</tr>
</tbody>
</table>

This database allows multiple destinations for the same MAC address. If the switch detects a new destination for an existing MAC entry, it just **adds** a new instance of that MAC to the table. This database allows only one destination for a MAC address. If the switch detects a new destination for an existing MAC entry, it **replaces** the existing MAC instance with a new instance showing the new destination.

Table 2-6 lists the database structure of current HP ProCurve switch models.
Table 2-6. Forwarding Database Structure for Managed HP ProCurve Switches

<table>
<thead>
<tr>
<th>Multiple Forwarding Databases*</th>
<th>Single Forwarding Database*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Series 5300XL switches</td>
<td>Switch 1600M/2400M/2424M-</td>
</tr>
<tr>
<td>Series 4100GL switches</td>
<td>Switch 4000M/8000M-</td>
</tr>
<tr>
<td>Series 2800 switches</td>
<td>Series 2500 switches-</td>
</tr>
<tr>
<td>Series 2600 switches</td>
<td>Switch 800T-</td>
</tr>
<tr>
<td>Switch 6108</td>
<td>Switch 2000-</td>
</tr>
</tbody>
</table>

*To determine whether other vendors’ devices use single-forwarding or multiple-forwarding database architectures, refer to the documentation provided for those devices.

Single Forwarding Database Operation

When a packet arrives with a destination MAC address that matches a MAC address in the the switch’s forwarding table, the switch tries to send the packet to the port listed for that MAC address. But, if the destination port is in a different VLAN than the VLAN on which the packet was received, the switch drops the packet. This is not a problem for a switch with a multiple forwarding database (refer to table 2-6, above) because the switch allows multiple instances of a given MAC address; one for each valid destination. However, a switch with a single forwarding database allows only one instance of a given MAC address. If you connect the two types of switches through multiple ports or trunks belonging to different VLANs, and enable routing on the Series 5300XL switch, then the other switch’s record of the port and VLAN on which the 5300XL exists can frequently change. This causes poor performance and the appearance of an intermittent or broken connection.
Example of an Unsupported Configuration and How To Correct It

The Problem. In figure 2-9, the MAC address table for Switch 8000M will sometimes record the 5308XL as accessed on port A1 (VLAN 1), and other times as accessed on port B1 (VLAN 2):

![Diagram showing VLAN configurations and forwarding databases]

1. The packet enters VLAN 1 in the Switch 8000 with the 5308XL's MAC address in the destination field. Because the 8000M has not yet learned this MAC address, it does not find the address in its address table, and floods the packet out all ports, including the VLAN 1 link (port “A1”) to the 5308XL. The 5308XL then routes the packet through the VLAN 2 link to the 8000M, which forwards the packet on to PC “B”. Because the 8000M received the packet from the 5308XL on VLAN 2 (port “B1”), the 8000M’s single forwarding database records the 5308XL as being on port “B1” (VLAN 2).

2. PC “A” now sends a second packet to PC “B”. The packet again enters VLAN 1 in the Switch 8000 with the 5308XL’s MAC address in the destination field. However, this time the Switch 8000M’s single forwarding database indicates that the 5308XL is on port B1 (VLAN 2), and the 8000M drops the packet instead of forwarding it.

3. Later, the 5308XL transmits a packet to the 8000M through the VLAN 1 link, and the 8000M updates its address table to indicate that the 5308XL is on port A1 (VLAN 1) instead of port B1 (VLAN 2). Thus, the 8000M’s information on the location of the 5308XL changes over time. For this
reason, the 8000M discards some packets directed through it for the 5308XL, resulting in poor performance and the appearance of an intermittent or broken link.

The Solution. To avoid the preceding problem, use only one cable or port trunk between the single-forwarding and multiple-forwarding database devices, and configure the link with multiple, tagged VLANs.

![Diagram showing the solution](image_url)

Figure 2-10. Example of a Solution for Single-Forwarding to Multiple-Forwarding Database Devices in a Multiple VLAN Environment

Now, the 8000M forwarding database always lists the 5308XL MAC address on port A1, and the 8000M will send traffic to either VLAN on the 5308X.

To increase the network bandwidth of the connection between the devices, you can use a trunk of multiple physical links rather than a single physical link.

Multiple Forwarding Database Operation

If you want to connect a Series 5300XL switch to another switch that has a multiple forwarding database, you can use either or both of the following connection options:

- A separate port or port trunk interface for each VLAN. This results in a forwarding database having multiple instances of the same MAC address with different VLAN IDs and port numbers. (See table 2-5.) The fact that the Series 5300XL Switch uses the same MAC address on all VLAN interfaces causes no problems.

- The same port or port trunk interface for multiple (tagged) VLANs. This results in a forwarding database having multiple instances of the same MAC address with different VLAN IDs, but the same port number.

Allowing multiple entries of the same MAC address on different VLANs enables topologies such as the following:
Configuring VLANS

Menu: Configuring Port-Based VLAN Parameters

The Menu interface enables you to configure and view port-based VLANS.

Note

The Menu interface configures and displays only port-based VLANS. The CLI configures and displays port-based and protocol-based VLANS (page 2-27).

In the factory default state, support is enabled for up to eight VLANS. (You can change the switch VLAN configuration to support up to 256 VLANS.) Also, all ports on the switch belong to the default VLAN (DEFAULT_VLAN) and are in the same broadcast/multicast domain. (The default VLAN is also the default Primary VLAN—see “The Primary VLAN” on page 2-43.) In addition to the default VLAN, you can configure up to 255 other static VLANS by changing the “Maximum VLANS” parameter, adding new VLAN names and VIDs, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 256 VLANS, including the default VLAN and any dynamic VLANS the switch creates if you enable GVRP—page 3-1.) Note that each port can be assigned to multiple VLANS by using VLAN tagging. (See “802.1Q VLAN Tagging” on page 2-38.)

To Change VLAN Support Settings

This section describes:

- Changing the maximum number of VLANS to support
Static Virtual LANs (VLANs)
Configuring VLANs

- Changing the Primary VLAN selection (See “Changing the Primary VLAN” on page 2-32.)
- Enabling or disabling dynamic VLANs (Refer to chapter 3, “GVRP”.)

1. From the Main Menu select:
   2. Switch Configuration
      8. VLAN Menu …
      1. VLAN Support

   You will then see the following screen:

   ![Image of VLAN Support screen]

   **Figure 2-12. The Default VLAN Support Screen**

   2. Press [E] (for Edit), then do one or more of the following:
   - To change the maximum number of VLANs, type the new number (1 - 256 allowed; default 8).
   - To designate a different VLAN as the Primary VLAN, select the Primary VLAN field and use the space bar to select from the existing options. (Note that the Primary VLAN must be a static, port-based VLAN.)
   - To enable or disable dynamic VLANs, select the GVRP Enabled field and use the Space bar to toggle between options. (For GVRP information, refer to chapter 3, “GVRP”.)

   **Note**

   For optimal switch memory utilization, set the number of VLANs at the number you will likely be using or a few more. If you need more VLANs later, you can increase this number, but a switch reboot will be required at that time.

3. Press [Enter] and then [S] to save the VLAN support configuration and return to the VLAN Menu screen.

   If you changed the value for Maximum VLANs to support, you will see an asterisk next to the VLAN Support option (see below).
An asterisk indicates you must reboot the switch to implement the new Maximum VLANs setting.

---

**Figure 2-13. VLAN Menu Screen Indicating the Need To Reboot the Switch**

- If you changed the VLAN Support option, you must reboot the switch before the Maximum VLANs change can take effect. You can go on to configure other VLAN parameters first, but remember to reboot the switch when you are finished.
- If you did not change the VLAN Support option, a reboot is not necessary.

4. Press [0] to return to the Main Menu.
Adding or Editing VLAN Names

Use this procedure to add a new VLAN or to edit the name of an existing VLAN.

1. From the Main Menu select:
   
   **2. Switch Configuration**
   
   **8. VLAN Menu ...**
   
   **2. VLAN Names**

   If multiple VLANs are not yet configured you will see a screen similar to figure 2-14:

   ![Fig. 2-14](default_vlan_names_screen.png)

   **Figure 2-14. The Default VLAN Names Screen**

2. Press [A] (for Add). You will then be prompted for a new VLAN name and VLAN ID:

   **802.1Q VLAN ID : 1**
   
   **Name : _**

3. Type in a VID (VLAN ID number). This can be any number from 2 to 4094 that is not already being used by another VLAN. (The switch reserves “1” for the default VLAN.)

   Remember that a VLAN *must* have the same VID in every switch in which you configure that same VLAN. (GVRP dynamically extends VLANs with correct VID numbering to other switches. Refer to chapter 3, “GVRP”.)

4. Press [↓] to move the cursor to the **Name** line and type the VLAN name (up to 12 characters, with no spaces) of a new VLAN that you want to add, then press [Enter].

   (Avoid these characters in VLAN names: 2, #, $, ^, &, *, {, and }.)

5. Press [S] (for Save). You will then see the VLAN Names screen with the new VLAN listed.
Static Virtual LANs (VLANs)
Configuring VLANs

Example of a New VLAN and ID

Figure 2-15. Example of VLAN Names Screen with a New VLAN Added

6. Repeat steps 2 through 5 to add more VLANs.

Remember that you can add VLANs until you reach the number specified in the Maximum VLANs to support field on the VLAN Support screen (see figure 2-12 on page 2-22). This includes any VLANs added dynamically due to GVRP operation.

7. Return to the VLAN Menu to assign ports to the new VLAN(s) as described in the next section, “Adding or Changing a VLAN Port Assignment”.

Adding or Changing a VLAN Port Assignment

Use this procedure to add ports to a VLAN or to change the VLAN assignment(s) for any port. (Ports not specifically assigned to a VLAN are automatically in the default VLAN.)

1. From the Main Menu select:
2. Switch Configuration
8. VLAN Menu …
3. VLAN Port Assignment

You will then see a VLAN Port Assignment screen similar to the following:

Note

The “VLAN Port Assignment” screen displays up to 32 static, port-based VLANs in ascending order, by VID. If the switch configuration includes more than 32 such VLANs, use the CLI show vlans [VID | ports <port-list>] command to list data on VLANs having VIDs numbered sequentially higher than the first 32.
Default: In this example, the "VLAN-22" has been defined, but no ports have yet been assigned to it. ("No" means the port is not assigned to that VLAN.)

Using GVRP? If you plan on using GVRP, any ports you don’t want to join should be changed to “Forbid”.

A port can be assigned to several VLANs, but only one of those assignments can be “Untagged”.

---

<table>
<thead>
<tr>
<th>Port</th>
<th>DEFAULT_VLAN</th>
<th>VLAN-22</th>
<th>Port</th>
<th>DEFAULT_VLAN</th>
<th>VLAN-22</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1</td>
<td>Untagged</td>
<td>No</td>
<td>a8</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>a2</td>
<td>Tagged</td>
<td>No</td>
<td>a9</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>a3</td>
<td>Untagged</td>
<td>No</td>
<td>a10</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>a4</td>
<td>Untagged</td>
<td>No</td>
<td>a11</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>a5</td>
<td>Untagged</td>
<td>No</td>
<td>a12</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>a6</td>
<td>Untagged</td>
<td>No</td>
<td>a13</td>
<td>Untagged</td>
<td>No</td>
</tr>
<tr>
<td>a7</td>
<td>Untagged</td>
<td>No</td>
<td>a14</td>
<td>Untagged</td>
<td>No</td>
</tr>
</tbody>
</table>

Actions: Cancel Edit Save Help

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

---

Figure 2-16. Example of the Port-Based VLAN Port Assignment Screen in the Menu Interface

2. To change a port’s VLAN assignment(s):
   b. Use the arrow keys to select a VLAN assignment you want to change.
   c. Press the Space bar to make your assignment selection (No, Tagged, Untagged, or Forbid).

Note

For GVRP Operation: If you enable GVRP on the switch, “No” converts to “Auto”, which allows the VLAN to dynamically join an advertised VLAN that has the same VID. See “Per-Port Options for Dynamic VLAN Advertising and Joining” on page 3-9.

Untagged VLANs: Only one untagged VLAN is allowed per port. Also, there must be at least one VLAN assigned to each port. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT_VLAN).

For example, if you want ports A4 and A5 to belong to both DEFAULT_VLAN and VLAN-22, and ports A6 and A7 to belong only to VLAN-22, you would use the settings in figure page 2-27. (This example assumes the default GVRP setting—disabled—and that you do not plan to enable GVRP later.)
Ports A4 and A5 are assigned to both VLANs. 
Ports A6 and A7 are assigned only to VLAN-22. 
All other ports are assigned only to the Default VLAN.

Figure 2-17. Example of Port-Based VLAN Assignments for Specific Ports

For information on VLAN tags (“Untagged” and “Tagged”), refer to “802.1Q VLAN Tagging” on page 2-38.

d. If you are finished assigning ports to VLANs, press [Enter] and then [S] (for Save) to activate the changes you’ve made and to return to the Configuration menu. (The console then returns to the VLAN menu.)

3. Return to the Main menu.

CLI: Configuring Port-Based and Protocol-Based VLAN Parameters

In the factory default state, all ports on the switch belong to the (port-based) default VLAN (DEFAULT_VLAN; VID = 1) and are in the same broadcast/multicast domain. (The default VLAN is also the Primary VLAN. For more on this topic, refer to “The Primary VLAN” on page 2-43.) You can configure up to 255 additional static VLANs by adding new VLAN names, and then assigning one or more ports to each VLAN. (The switch accepts a maximum of 256 VLANs, including the default VLAN and any dynamic VLANs the switch creates if you enable GVRP. Refer to chapter 3, “GVRP”.) Note that each port can be assigned to multiple VLANs by using VLAN tagging. (See “802.1Q VLAN Tagging” on page 2-38.)
### VLAN Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show vlans</td>
<td>below-</td>
</tr>
<tr>
<td>show vlan &lt; vid &gt;</td>
<td>2-30-</td>
</tr>
<tr>
<td>max-vlans &lt;1-256&gt;</td>
<td>2-31-</td>
</tr>
<tr>
<td>primary-vlan &lt; vid &gt;</td>
<td>2-32-</td>
</tr>
<tr>
<td>[no] vlan &lt; vid &gt;</td>
<td>2-33-</td>
</tr>
<tr>
<td>auto &lt; port-list &gt;</td>
<td>2-36 (Available if GVRP enabled.)-</td>
</tr>
<tr>
<td>forbid</td>
<td>2-36-</td>
</tr>
<tr>
<td>name &lt; vlan-name &gt;</td>
<td>2-36-</td>
</tr>
<tr>
<td>protocol &lt; protocol-list &gt;</td>
<td>2-33-</td>
</tr>
<tr>
<td>tagged &lt; port-list &gt;</td>
<td>2-36-</td>
</tr>
<tr>
<td>untagged &lt; port-list &gt;</td>
<td>2-36-</td>
</tr>
<tr>
<td>voice</td>
<td>2-49-</td>
</tr>
<tr>
<td>static-vlan &lt; vlan-id &gt;</td>
<td>2-34 (Available if GVRP enabled.)-</td>
</tr>
</tbody>
</table>

### Displaying the Switch’s VLAN Configuration.

The `show vlans` command lists the VLANs currently running in the switch, with VID, VLAN name, and VLAN status. Dynamic VLANs appear only if the switch is running with GVRP enabled and one or more ports has dynamically joined an advertised VLAN. (In the default configuration, GVRP is disabled. (Refer to chapter 3, “GVRP”.)

**Syntax:** show vlans

**Maximum VLANs to support:** Shows the number of VLANs the switch can currently support. (Default: 8; Maximum: 256)

**Primary VLAN:** Refer to “The Primary VLAN” on page 2-43.

**Management VLAN:** Refer to “The Secure Management VLAN” on page 2-44.

**802.1Q VLAN ID:** The VLAN identification number, or VID. Refer to “Terminology” on page 2-5.

**Name:** The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of **VLAN-x** where “x” matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of **GVRP_x** where “x” matches the applicable VID.
Static Virtual LANs (VLANs)

Configuring VLANs

Status:

**Port-Based**: Port-Based, static VLAN

**Protocol**: Protocol-Based, static VLAN

**Dynamic**: Port-Based, temporary VLAN learned through GVRP (Refer to chapter 3, “GVRP”.)

**Voice**: Indicates whether a (port-based) VLAN is configured as a voice VLAN. Refer to “Voice VLANs” on page 2-49.

For example:

```
HPswitch# show vlans

Status and Counters - VLAN Information

Maximum VLANs to support : 8
Primary VLAN : DEFAULT_VLAN
Management VLAN :

802.1Q VLAN ID  Name         | Status     Voice
-------------------+------------+-----
  1     DEFAULT_VLAN | Port-based No
 10     VLAN_10     | Port-based Yes
 20     VLAN_20     | Protocol   No
 33     GVRP_33     | Dynamic    No

Figure 2-18. Example of “Show VLAN” Listing (GVRP Enabled)
```

When GVRP is disabled (the default), Dynamic VLANs do not exist on the switch and do not appear in this listing. (Refer to chapter 3, “GVRP”.)
Displaying the Configuration for a Particular VLAN. This command uses the VID to identify and display the data for a specific static or dynamic VLAN.

Syntax: show vlans < vlan-id >

802.1Q VLAN ID: The VLAN identification number, or VID. Refer to “Terminology” on page 2-5.

Name: The default or specified name assigned to the VLAN. For a static VLAN, the default name consists of VLAN-x where “x” matches the VID assigned to that VLAN. For a dynamic VLAN, the name consists of GVRP_x where “x” matches the applicable VID.

Status:

Port-Based: Port-Based, static VLAN

Protocol: Protocol-Based, static VLAN

Dynamic: Port-Based, temporary VLAN learned through GVRP (Refer to the chapter titled “GVRP” in the Advanced Traffic Management Guide for your switch.)

Voice: Indicates whether a (port-based) VLAN is configured as a voice VLAN. Refer to “Voice VLANs” on page 2-49.

Port Information: Lists the ports configured as members of the VLAN.

DEFAULT: Shows whether a port is a tagged or untagged member of the listed VLAN.

Unknown VLAN: Shows whether the port can become a dynamic member of an unknown VLAN for which it receives an advertisement. GVRP must be enabled to allow dynamic joining to occur. Refer to table 3-1 on page 3-8.

Status: Shows whether the port is participating in an active link.
Static Virtual LANs (VLANs)  
Configuring VLANs

Figure 2-19. Example of “Show VLAN” for a Specific Static VLAN

<table>
<thead>
<tr>
<th>Port Information</th>
<th>DEFAULT</th>
<th>Unknown VLAN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A12</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
</tr>
<tr>
<td>A13</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
</tr>
<tr>
<td>A14</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
</tr>
<tr>
<td>A15</td>
<td>Untagged</td>
<td>Learn</td>
<td>Down</td>
</tr>
<tr>
<td>A16</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
</tr>
<tr>
<td>A17</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
</tr>
<tr>
<td>A18</td>
<td>Untagged</td>
<td>Learn</td>
<td>Up</td>
</tr>
</tbody>
</table>

Show VLAN lists this data when GVRP is enabled and at least one port on the switch has dynamically joined the designated VLAN.

Figure 2-20. Example of “Show VLAN” for a Specific Dynamic VLAN

<table>
<thead>
<tr>
<th>Port Information</th>
<th>DEFAULT</th>
<th>Unknown VLAN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A6</td>
<td>Auto</td>
<td>Learn</td>
<td>Up</td>
</tr>
</tbody>
</table>

Changing the Number of VLANs Allowed on the Switch. In the default VLAN configuration, the switch allows a maximum of 8 VLANs. You can specify any value from 1 to 256.

Syntax: max-vlans < 1-256 >

Specifies the maximum number of VLANs to allow. (If GVRP is enabled, this setting includes any dynamic VLANs on the switch.) As part of implementing a new setting, you must execute a write memory command (to save the new value to the startup-config file) and then reboot the switch.

Note: If multiple VLANs exist on the switch, you cannot reset the maximum number of VLANs to a value smaller than the current number of VLANs.
For example, to reconfigure the switch to allow 10 VLANs:

HPswitch(config)# max-vlans 10
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# boot
Device will be rebooted, do you want to continue [y/n]? y

Figure 2-21. Example of Command Sequence for Changing the Number of VLANs

**Changing the Primary VLAN.** In the default VLAN configuration, the port-based default VLAN (DEFAULT_VLAN) is the Primary VLAN. However, you can reassign the Primary VLAN to any port-based, static VLAN on the switch. (For more on the Primary VLAN, refer to “The Primary VLAN” on page 2-43.) To identify the current Primary VLAN and list the available VLANs and their respective VIDs, use `show vlans`.

**Syntax:** `primary-vlan < vid | ascii-name-string >`

*Reassigns the Primary VLAN function. Re-assignment must be to an existing, port-based, static VLAN. (The switch will not reassign the Primary VLAN function to a protocol VLAN.) If you re-assign the Primary VLAN to a non-default VLAN, you cannot later delete that VLAN from the switch until you again re-assign the Primary VLAN to another port-based, static VLAN.*

For example, if you wanted to reassign the Primary VLAN to VLAN 22 and rename the VLAN with “22-Primary” and display the result:

```
HP ProCurve Switch 5304XL(config)# primary-vlan 22
HP ProCurve Switch 5304XL(config)# vlan 22 name 22-Primary
HP ProCurve Switch 5304XL(config)# show vlans

Status and Counters - VLAN Information

Maximum VLANs to support : 8
Primary VLAN : 22-Primary
Management VLAN :

802.1Q VLAN ID Name Status VOIP Capable
--------------- --------------- ---------------
1 DEFAULT_VLAN Static          
22 22-Primary Static
```

Figure 2-22. Example of Reassigning Primary VLAN and Changing the VLAN Name
Creating a New Static VLAN (Port-Based or Protocol-Based)

Changing the VLAN Context Level.

The `vlan <vid>` command operates in the global configuration context to either configure a static VLAN and/or take the CLI to the specified VLAN’s context.

**Syntax:** `[ no ] vlan < vid | ascii-name-string >`

*If < vid > does not exist in the switch, this command creates a port-based VLAN with the specified < vid >. If the command does not include options, the CLI moves to the newly created VLAN context. If you do not specify an optional VLAN name, the switch assigns a name in the default name format: VLANn where n is the < vid > assigned to the VLAN. If the VLAN already exists and you enter either the vid or the ascii-name-string, the CLI moves to the specified VLAN’s context.*

*The [no] form without options deletes the VLAN if no ports are members of the VLAN or if any member ports also belong to another VLAN.*

`[ protocol < ipx | ipv4 | ipv6 | arp | appletalk | sna | declat | netbeui > ]`

*Configures a static, protocol VLAN of the specified type. If there are multiple protocols configured in the VLAN, then the [no] form removes the specified protocol from the VLAN. If a protocol VLAN is configured with only one protocol type and you use the [no] form of this command to remove that protocol type, the switch changes the protocol VLAN to a port-based VLAN if the VLAN does not include an untagged member port. (If an untagged member port exists on the protocol VLAN, you must either convert the port to a tagged member or remove the port from the VLAN before removing the last protocol type from the VLAN.)*

**Note:** If you create an IPv4 protocol VLAN, you must also assign the ARP protocol option to the VLAN to provide IP address resolution. Otherwise, IP packets are not deliverable. A “Caution” message appears in the CLI if you configure IPv4 in protocol VLAN that does not already include the arp protocol option. The same message appears if you add or delete another protocol in the same VLAN.
name < ascii-name-string >

When included in a vlan command for creating a new static VLAN, specifies a non-default VLAN name. Also used to change the current name of an existing VLAN. (Avoid spaces and the following characters in the <ascii-name-string> entry: @, #, $, ^, &, *, (, and ). To include a blank space in a VLAN name, enclose the name in single or double quotes (‘...’ or “…”).

[voice]

Designates a VLAN for VoIP use. For more on this topic, refer to “Voice VLANs” on page 2-49.

For example, to create a new, port-based, static VLAN with a VID of 100:

```
HPswitch(config)# vlan 100
HPswitch(vlan-100)# show vlans
Status and Counters - VLAN Information
 Maximum VLANs to support : 8
 Primary VLAN : DEFAULT_VLAN
 Management VLAN

  802.1Q VLAN ID  Name           Status     Voice
     --------  -------          --------
     1       DEFAULT_VLAN     Port-based No
     100      VLAN100          Port-based No

Figure 2-23. Example of Creating a New, Port-Based, Static VLAN
```

To go to a different VLAN context level, such as to the default VLAN:

```
HPswitch(vlan-100)# vlan default_vlan
HPswitch(vlan-1) _
```

Converting a Dynamic VLAN to a Static VLAN. Use this feature if you want to convert a dynamic, port-based VLAN membership to a static, port-based VLAN membership. This is necessary if you want to make the VLAN permanent on the switch.
Syntax: static-vlan < vlan-id >

Converts a dynamic, port-based VLAN membership to a static, port-based VLAN membership. (Allows port-based VLANs only). For this command, < vlan-id > refers to the VID of the dynamic VLAN membership. (Use show vlan to help identify the VID you need to use.) This command requires that GVRP is running on the switch and a port is currently a dynamic member of the selected VLAN. After you convert a dynamic VLAN to static, you must configure the switch's per-port participation in the VLAN in the same way that you would for any static VLAN. (For GVRP and dynamic VLAN operation, refer to chapter 3, “GVRP”.)

For example, suppose a dynamic VLAN with a VID of 125 exists on the switch. The following command converts the VLAN to a port-based, static VLAN.

HPswitch(config)# static-vlan 125
Configuring Static VLAN Per-Port Settings. The `vlan <vlan-id>` command, used with the options listed below, changes the name of an existing static VLAN and changes the per-port VLAN membership settings.

**Note**
You can use these options from the configuration level by beginning the command with `vlan <vid>`, or from the context level of the specific VLAN by just typing the command option.

**Syntax:** `[no] vlan <vid> [tagged <port-list> | untagged <port-list> | forbid <port-list> | auto <port-list>]`

- **tagged <port-list>**
  Configures the indicated port(s) as Tagged for the specified VLAN. The “no” version sets the port(s) to either No or (if GVRP is enabled) to Auto.

- **untagged <port-list>**
  Configures the indicated port(s) as Untagged for the specified VLAN. The “no” version sets the port(s) to either No or (if GVRP is enabled) to Auto.

- **forbid <port-list>**
  Used in port-based VLANs to configure <port-list> as “forbidden” to become a member of the specified VLAN, as well as other actions. Does not operate with protocol VLANs. The “no” version sets the port(s) to either No or (if GVRP is enabled) to Auto. Refer to the chapter titled “GVRP” in the Advanced Traffic Management Guide for your switch.

- **auto <port-list>**
  Available if GVRP is enabled on the switch. Returns the per-port settings for the specified VLAN to Auto operation. Note that Auto is the default per-port setting for a static VLAN if GVRP is running on the switch. (For information on dynamic VLAN and GVRP operation, refer to the chapter titled “GVRP” in the Advanced Traffic Management Guide for your switch.)

For example, suppose you have a VLAN named VLAN100 with a VID of 100, and all ports are set to No for this VLAN. To change the VLAN name to “Blue_Team” and set ports A1 - A5 to Tagged, you would use these commands:

```
HPswitch(config)# vlan 100 name Blue_Team
HPswitch(config)# vlan 100 tagged a1-a5
```

To move to the vlan 100 context level and execute the same commands:
Static Virtual LANs (VLANs)

Configuring VLANs

HPswitch(config)# vlan 100
HPswitch(vlan-100)# name Blue_Team
HPswitch(vlan-100)# tagged a1-a5

Similarly, to change the tagged ports in the above examples to No (or Auto, if GVRP is enabled), you could use either of the following commands.

At the global config level, use:

HPswitch(config)# no vlan 100 tagged a1-a5

- or -

At the VLAN 100 context level, use:

HPswitch(vlan-100)# no tagged a1-a5

---

Note

You cannot use these commands with dynamic VLANs. Attempting to do so results in the message "VLAN already exists." and no change occurs.

Web: Viewing and Configuring VLAN Parameters

In the web browser interface you can do the following:

- Add VLANs
- Rename VLANs
- Remove VLANs
- Configure VLAN tagging mode per-port
- Configure GVRP mode
- Select a new Primary VLAN

To configure other static VLAN port parameters, you will need to use either the CLI or the menu interface (available by Telnet from the web browser interface).

1. Click on the Configuration tab.
2. Click on [Vlan Configuration].
3. Click on [Add/Remove VLANs].

For web-based Help on how to use the web browser interface screen, click on the [?] button provided on the web browser screen.
802.1Q VLAN Tagging

General Applications:

- The switch requires VLAN tagging on a given port if more than one VLAN of the same type uses the port. When a port belongs to two or more VLANs of the same type, they remain as separate broadcast domains and cannot receive traffic from each other without routing. (If multiple, non-routable VLANs exist in the switch—such as SNA protocol VLANs—then they cannot receive traffic from each other under any circumstances.)

- The switch requires VLAN tagging on a given port if the port will be receiving inbound, tagged VLAN traffic that should be forwarded. Even if the port belongs to only one VLAN, it forwards inbound tagged traffic only if it is a tagged member of that VLAN.

- If the only authorized, inbound VLAN traffic on a port arrives untagged, then the port must be an untagged member of that VLAN. This is the case where the port is connected to a non 802.1Q-compliant device or is assigned to only one VLAN.

For example, if port 7 on an 802.1Q-compliant switch is assigned to only the Red VLAN, the assignment can remain “untagged” because the port will forward traffic only for the Red VLAN. However, if both the Red and Green VLANs are assigned to port 7, then at least one of those VLAN assignments must be “tagged” so that Red VLAN traffic can be distinguished from Green VLAN traffic. Figure 2-24 shows this concept:
In switch X:
- VLANs assigned to ports X1 - X6 can all be untagged because there is only one VLAN assignment per port. Red VLAN traffic will go out only the Red ports; Green VLAN traffic will go out only the Green ports, and so on. Devices connected to these ports do not have to be 802.1Q-compliant.
- However, because both the Red VLAN and the Green VLAN are assigned to port X7, at least one of the VLANs must be tagged for this port.

In switch Y:
- VLANs assigned to ports Y1 - Y4 can all be untagged because there is only one VLAN assignment per port. Devices connected to these ports do not have to be 802.1Q-compliant.
- Because both the Red VLAN and the Green VLAN are assigned to port Y5, at least one of the VLANs must be tagged for this port.

In both switches: The ports on the link between the two switches must be configured the same. As shown in figure 2-24 (above), the Red VLAN must be untagged on port X7 and Y5 and the Green VLAN must be tagged on port X7 and Y5, or vice-versa.
Each 802.1Q-compliant VLAN must have its own unique VID number, and that VLAN must be given the same VID in every device in which it is configured. That is, if the Red VLAN has a VID of 10 in switch X, then 10 must also be used for the Red VID in switch Y.

VLAN tagging gives you several options:

- Since the purpose of VLAN tagging is to allow multiple VLANs on the same port, any port that has only one VLAN assigned to it can be configured as “Untagged” (the default) if the authorized inbound traffic for that port arrives untagged.
- Any port with two or more VLANs of the same type can have one such VLAN assigned as “Untagged”. All other VLANs of the same type must be configured as “Tagged”. That is:

<table>
<thead>
<tr>
<th>Port-Based VLANs</th>
<th>Protocol VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged.</td>
<td>A port can be an untagged member of one protocol-based VLAN of each protocol type. When assigning a port to multiple, protocol-based VLANs sharing the same type, the port can be an untagged member of only one such VLAN.</td>
</tr>
<tr>
<td>A port can be a tagged member of any port-based VLAN. See above.</td>
<td>A port can be a tagged member of any protocol-based VLAN. See above.</td>
</tr>
</tbody>
</table>

Note: A given VLAN must have the same VID on all 802.1Q-compliant devices in which the VLAN occurs. Also, the ports connecting two 802.1Q devices should have identical VLAN configurations.
If all end nodes on a port comply with the 802.1Q standard and are configured to use the correct VID, then, you can configure all VLAN assignments on a port as “Tagged” if doing so either makes it easier to manage your VLAN assignments, or if the authorized, inbound traffic for all VLANs on the port will be tagged.

For a summary and flowcharts of untagged and tagged VLAN operation on inbound traffic, refer to the following under “VLAN Operating Rules” on pages 2-13 through 2-16:

- “Inbound Tagged Packets”
- “Untagged Packet Forwarding” and figure 2-7
- “Tagged Packet Forwarding” and figure 2-8

**Example.** In the following network, switches X and Y and servers S1, S2, and the AppleTalk server are 802.1Q-compliant. (Server S3 could also be 802.1Q-compliant, but it makes no difference for this example.) This network includes both protocol-based (AppleTalk) VLANs and port-based VLANs.

![Diagram](image-url)
The VLANs assigned to ports X4 - X6, Y2 - Y5 can all be untagged because there is only one VLAN assigned per port.

Port X1 has two AppleTalk VLANs assigned, which means that one VLAN assigned to this port can be untagged and the other must be tagged.

Ports X2 and Y1 have two port-based VLANs assigned, so one can be untagged and the other must be tagged on both ports.

Ports X3 and Y6 have two port-based VLANs and one protocol-based VLAN assigned. Thus, one port-based VLAN assigned to this port can be untagged and the other must be tagged. Also, since these two ports share the same link, their VLAN configurations must match.

<table>
<thead>
<tr>
<th>Port</th>
<th>AT-1 VLAN</th>
<th>AT-2 VLAN</th>
<th>Red VLAN</th>
<th>Green VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>X1</td>
<td>Untagged</td>
<td>Tagged</td>
<td>No*</td>
<td>No*</td>
</tr>
<tr>
<td>X2</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
<td>Tagged</td>
</tr>
<tr>
<td>X3</td>
<td>No*</td>
<td>Untagged</td>
<td>Untagged</td>
<td>Tagged</td>
</tr>
<tr>
<td>X4</td>
<td>No*</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
</tr>
<tr>
<td>X5</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
<td>No*</td>
</tr>
<tr>
<td>X6</td>
<td>Untagged</td>
<td>No*</td>
<td>No*</td>
<td>No*</td>
</tr>
<tr>
<td>Y1</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
<td>Tagged</td>
</tr>
<tr>
<td>Y2</td>
<td>No*</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
</tr>
<tr>
<td>Y3</td>
<td>No*</td>
<td>Untagged</td>
<td>No*</td>
<td>No*</td>
</tr>
<tr>
<td>Y4</td>
<td>No*</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
</tr>
<tr>
<td>Y5</td>
<td>No*</td>
<td>No*</td>
<td>Untagged</td>
<td>No*</td>
</tr>
<tr>
<td>Y6</td>
<td>No</td>
<td>Untagged</td>
<td>Untagged</td>
<td>Tagged</td>
</tr>
</tbody>
</table>

**No** means the port is not a member of that VLAN. For example, port X3 is not a member of the Red VLAN and does not carry Red VLAN traffic. Also, if GVRP were enabled (port-based only), “Auto” would appear instead of “No”.

**Note**

VLAN configurations on ports connected by the same link must match. Because ports X2 and Y5 are opposite ends of the same point-to-point connection, both ports must have the same VLAN configuration; that is, both ports configure the Red VLAN as “Untagged” and the Green VLAN as “Tagged”.

---

2-42
Special VLAN Types

VLAN Support and the Default VLAN

In the factory default configuration, VLAN support is enabled and all ports on the switch belong to the port-based, default VLAN (named DEFAULT_VLAN). This places all ports in the switch into one physical broadcast domain. In the factory-default state, the default VLAN is also the Primary VLAN.

You can partition the switch into multiple virtual broadcast domains by configuring one or more additional VLANs and moving ports from the default VLAN to the new VLANs. (The switch supports up to 256 static and dynamic VLANs.) You can change the name of the default VLAN, but you cannot change the default VLAN’s VID (which is always “1”). Although you can remove all ports from the default VLAN (by placing them in another port-based VLAN), this VLAN is always present; that is, you cannot delete it from the switch.

For details on port VLAN settings, refer to “Configuring Static VLAN Per-Port Settings” on page 2-36.

The Primary VLAN

Because certain features and management functions run on only one VLAN in the switch, and because DHCP and Bootp can run per-VLAN, there is a need for a dedicated VLAN to manage these features and ensure that multiple instances of DHCP or Bootp on different VLANs do not result in conflicting configuration values for the switch. The Primary VLAN is the VLAN the switch uses to run and manage these features and data. In the factory-default configuration, the switch designates the default VLAN (DEFAULT_VLAN; VID = 1) as the Primary VLAN. However, to provide more control in your network, you can designate another static, port-based VLAN as primary. To summarize, designating a non-default VLAN as primary means that:

- The switch reads DHCP responses on the Primary VLAN instead of on the default VLAN. (This includes such DHCP-resolved parameters as the TimeP server address, Default TTL, and IP addressing—including the Gateway IP address—when the switch configuration specifies DHCP as the source for these values.)

- The default VLAN continues to operate as a standard VLAN (except, as noted above, you cannot delete it or change its VID).

- Any ports not specifically assigned to another VLAN will remain assigned to the Default VLAN, regardless of whether it is the Primary VLAN.
Static Virtual LANs (VLANs)

Special VLAN Types

Candidates for Primary VLAN include any static, port-based VLAN currently configured on the switch. (Protocol-Based VLANs and dynamic—GVRP-learned—VLANs that have not been converted to a static VLAN cannot be the Primary VLAN.) To display the current Primary VLAN, use the CLI `show vlan` command.

**Note**

If you configure a non-default VLAN as the Primary VLAN, you cannot delete that VLAN unless you first select a different VLAN to serve as primary.

If you manually configure a gateway on the switch, it ignores any gateway address received via DHCP or Bootp.

To change the Primary VLAN configuration, refer to “Changing the Primary VLAN” on page 2-32.

The Secure Management VLAN

Configuring a secure Management VLAN creates an isolated network for managing the HP ProCurve switches that support this feature. (As of February, 2004, the Secure Management VLAN feature is available on these HP ProCurve switches:

- Switch 6108
- 5300XL Series
- 4100GL Series
- 2800 Series
- 2600 Series

If you configure a Secure Management VLAN, access to the VLAN and to the switch’s management functions (Menu, CLI, and web browser interface) is available only through ports configured as members.

- Multiple ports on the switch can belong to the Management VLAN. This allows connections for multiple management stations you want to have access to the Management VLAN, while at the same time allowing Management VLAN links between switches configured for the same Management VLAN.

- Only traffic from the Management VLAN can manage the switch, which means that only the workstations and PCs connected to ports belonging to the Management VLAN can manage and reconfigure the switch.

Figure 2-27 illustrates use of the Management VLAN feature to support management access by a group of management workstations.
The Secure Management VLAN must be a static, port-based VLAN with a manually configured IP address and subnet mask. (The switch does not allow the Management VLAN to acquire IP addressing through DHCP/Bootp.)

- Switches “A”, “B”, and “C” are connected by ports belonging to the management VLAN.
- Hub “X” is connected to a switch port that belongs to the management VLAN. As a result, the devices connected to Hub X are included in the management VLAN.
- Other devices connected to the switches through ports that are not in the management VLAN are excluded from management traffic.

Figure 2-27. Example of Potential Security Breaches

In figure 2-28, Workstation 1 has management access to all three switches through the Management VLAN, while the PCs do not. This is because configuring a switch to recognize a Management VLAN automatically excludes attempts to send management traffic from any other VLAN.
Static Virtual LANs (VLANs)
Special VLAN Types

Links with Ports Configured as Members of the Management VLAN and other VLANs

Links Not Belonging to the Management VLAN

System Management Workstation

Figure 2-28. Example of Management VLAN Control in a LAN

Table 2-7. VLAN Membership in Figure 2-28

<table>
<thead>
<tr>
<th>Switch</th>
<th>A1</th>
<th>A3</th>
<th>A6</th>
<th>A7</th>
<th>B2</th>
<th>B4</th>
<th>B5</th>
<th>B9</th>
<th>C2</th>
<th>C3</th>
<th>C6</th>
<th>C8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VLAN (VID = 7)</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>Marketing VLAN (VID = 12)</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Shipping Dept. VLAN (VID = 20)</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
<td>N</td>
</tr>
<tr>
<td>DEFAULT-VLAN (VID = 1)</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Preparation

1. Determine a VID and VLAN name suitable for your Management VLAN.
   (You must manually configure the IP addressing for the Management VLAN. The switch does not allow the Management VLAN to acquire an IP address through DHCP/Bootp.)

2. Plan your Management VLAN topology to use HP ProCurve switches that support this feature. (Refer to page 2-44.) The ports belonging to the Management VLAN should be only the following:
   - Ports to which you will connect authorized management stations (such as Port A7 in figure 2-28.)
   - Ports on one switch that you will use to extend the Management VLAN to ports on other HP ProCurve switches (such as ports A1 and B2 or B4 and C2 in figure 2-28 on page 2-46.).
Hubs dedicated to connecting management stations to the Management VLAN can also be included in the above topology. Note that any device connected to a hub in the Management VLAN will also have Management VLAN access.

3. Configure the Management VLAN on the selected switch ports.

4. Test the management VLAN from all of the management stations authorized to use the Management VLAN, including any SNMP-based network management stations. Ensure that you include testing any Management VLAN links between switches.

**Note**

If you configure a Management VLAN on a switch by using a Telnet connection through a port that is not in the Management VLAN, then you will lose management contact with the switch if you log off your Telnet connection or execute **write memory** and **reboot** the switch.

**Configuration**

**Syntax:** [no] management-vlan <vlan-id | vlan-name>

*Configures an existing VLAN as the management VLAN. The no form disables the management VLAN and returns the switch to its default management operation. Default: Disabled. In this case, the VLAN returns to standard VLAN operation.*

For example, suppose you have already configured a VLAN named **My_VLAN** with a VID of 100 in a Series 5300XL switch. Now you want to configure the switch to do the following:

- Use **My_VLAN** as a Management VLAN (tagged, in this case) to connect port A1 on switch “A” to a management station. (The management station includes a network interface card with 802.1Q tagged VLAN capability.)
- Use port A2 to extend the Management VLAN to port B1 (which is already configured as a tagged member of **My_VLAN**) on an adjacent Series 5300XL switch.

![Figure 2-29. Illustration of Configuration Example](image-url)
Static Virtual LANs (VLANs)
Special VLAN Types

Deleting the Management VLAN

You can disable the Secure Management feature without deleting the VLAN itself. For example, either of the following commands disables the Secure Management feature in the above example:

HPswitch (config)# no management-vlan 100
HPswitch (config)# no management-vlan my_vlan

Operating Notes for Management VLANs

- Use only a static, port-based VLAN for the Management VLAN.
- The Management VLAN does not support IGMP operation.
- On Series 5300XL switches with routing enabled, routing between the Management VLAN and other VLANs is not allowed.
- If there are more than 25 VLANs configured on the switch, reboot the switch after configuring the management VLAN. (HP Series 5300XL switches only.)
- If you implement a Management VLAN in a switch mesh environment, all meshed ports on Series 5300XL switches will be members of the Management VLAN.
- Only one Management-VLAN can be active in the switch. If one Management-VLAN VID is saved in the startup-config file and you configure a different VID in the running-config file, the switch uses the running-config version until you either use the write-memory command or reboot the switch.
- During a Telnet session to the switch, if you configure the Management-VLAN to a VID that excludes the port through which you are connected to the switch, you will continue to have access only until you terminate the session by logging out or rebooting the switch.
- During a web browser session to the switch, if you configure the Management-VLAN to a VID that excludes the port through which you are connected to the switch, you will continue to have access only until you close the browser session or rebooting the switch.

Note

The Management-VLAN feature does not control management access through a direct connection to the switch’s serial port.
Enabling Spanning Tree where there are multiple links using separate VLANs, including the Management VLAN, between a pair of switches, Spanning Tree will force the blocking of one or more links. This may include the link carrying the Management VLAN, which will cause loss of management access to some devices. This can also occur where meshing is configured and the Management VLAN is configured on a separate link.

**Figure 2-30. Example of Inadvertently Blocking a Management VLAN Link by Implementing Spanning Tree**

**Voice VLANs**

Configuring voice VLANs separates voice traffic from data traffic and shields your voice traffic from broadcast storms. This section describes how to configure the switch for voice VLAN operation.

**Operating Rules for Voice VLANs**

- You must statically configure voice VLANs. GVRP and dynamic VLANs do not support voice VLAN operation.
- Configure all ports in a voice VLAN as tagged members of the VLAN. This ensures retention of the QoS (Quality of Service) priority included in voice VLAN traffic moving through your network.
Static Virtual LANs (VLANs)
Special VLAN Types

If a telephone connected to a voice VLAN includes a data port used for connecting other networked devices (such as PCs) to the network, then you must configure the port as a tagged member of the voice VLAN and a tagged or untagged member of the data VLAN you want the other networked device to use.

Components of Voice VLAN Operation

■ **Voice VLAN(s):** Configure one or more voice VLANs on the switch. Some reasons for having multiple voice VLANs include:
  • Employing telephones with different VLAN requirements
  • Better control of bandwidth usage
  • Segregating telephone groups used for different, exclusive purposes

Where multiple voice VLANs exist on the switch, you can use routing to communicate between telephones on different voice VLANs.

■ **Tagged/Untagged VLAN Membership:** If the appliances using a voice VLAN transmit tagged VLAN packets, then configure the member ports as tagged members of the VLAN. Otherwise, configure the ports as untagged members.

Voice VLAN QoS Prioritizing (Optional)

Without configuring the switch to prioritize voice VLAN traffic, one of the following conditions applies:

■ If the ports in a voice VLAN are not tagged members, then the switch forwards all traffic on that VLAN at “normal” priority.

■ If the ports in a voice VLAN are tagged members, then the switch forwards all traffic on that VLAN at whatever priority the traffic has when received inbound on the switch.

Using the switch’s QoS VLAN-ID (VID) Priority option, you can change the priority of voice VLAN traffic moving through the switch. If all port memberships on the voice VLAN are tagged, the priority level you set for voice VLAN traffic is carried to the next device. With all ports on the voice VLAN configured as tagged members, you can enforce a QoS priority policy moving through the switch and through your network. To set a priority on a voice VLAN, use the following command:

**Syntax:** `vlan < vid > qos priority < 0 - 7 >`

*The qos priority default setting is 0 (normal), with 1 as the lowest priority and 7 as the highest priority.*
For example, if you configured a voice VLAN with a VID of 10, and wanted the highest priority for all traffic on this VLAN, you would execute the following command:

```
HPswitch (config) # vlan 10 qos priority 7
HPswitch (config) # write memory
```

Note that you also have the option of resetting the DSCP (DiffServe Code-point) on tagged voice VLAN traffic moving through the switch. For more on this and other QoS topics, refer to the chapter titled “Quality of Service (QoS): Managing Bandwidth More Effectively”.

Voice VLAN Access Security

You can use port security configured on an individual port or group of ports in a voice VLAN. That is, you can allow or deny access to a phone having a particular MAC address. Refer to chapter titled “Configuring and Monitoring Port Security” in the Access Security Guide (p/n 5990-6052, February 2004 or a later version).

**Note**

MAC authentication is not recommended in voice VLAN applications.

Effect of VLANs on Other Switch Features

Spanning Tree Operation with VLANs

Depending on the spanning-tree option configured on the switch, the spanning-tree feature may operate as a single instance across all ports on the switch (regardless of VLAN assignments) or multiple instance on a per-VLAN basis. For single-instance operation, this means that if redundant physical links exist between the switch and another 802.1Q device, all but one link will be blocked, regardless of whether the redundant links are in separate VLANs. In this case you can use port trunking to prevent Spanning Tree from unnecessarily blocking ports (and to improve overall network performance). For multiple-instance operation, physically redundant links belonging to different VLANs can remain open. Refer to chapter 6, “Spanning-Tree Operation”.
Note that Spanning Tree operates differently in different devices. For example, in the (obsolete, non-802.1Q) HP Switch 2000 and the HP Switch 800T, Spanning Tree operates on a per-VLAN basis, allowing redundant physical links as long as they are in separate VLANs.

**IP Interfaces**

There is a one-to-one relationship between a VLAN and an IP network interface. Since the VLAN is defined by a group of ports, the state (up/down) of those ports determines the state of the IP network interface associated with that VLAN. When a port-based VLAN or an IPv4 or IPv6 protocol-based VLAN comes up because one or more of its ports is up, the IP interface for that VLAN is also activated. Likewise, when a VLAN is deactivated because all of its ports are down, the corresponding IP interface is also deactivated.

**VLAN MAC Address**

A Series 5300XL switch has one unique MAC address for all of its VLAN interfaces. You can send an 802.2 test packet to this MAC address to verify connectivity to the switch. Likewise, you can assign an IP address to the VLAN interface, and when you Ping that address, ARP will resolve the IP address to this single MAC address. In a topology where a Switch Series 5300XL device has multiple VLANs and must be connected to a device having a single forwarding database, such as the Switch 4000M, some cabling restrictions apply. For more on this topic, refer to “Multiple VLAN Considerations” on page 2-17.

**Port Trunks**

When assigning a port trunk to a VLAN, all ports in the trunk are automatically assigned to the same VLAN. You cannot split trunk members across multiple VLANs. Also, a port trunk is tagged, untagged, or excluded from a VLAN in the same way as for individual, untrunked ports.

**Port Monitoring**

If you designate a port on the switch for network monitoring, this port will appear in the Port VLAN Assignment screen and can be configured as a member of any VLAN. For information on how broadcast, multicast, and unicast packets are tagged inside and outside of the VLAN to which the monitor port is assigned, refer to the section titled “VLAN-Related Problems” in the “Troubleshooting” chapter of the Management and Configuration Guide for your switch.
VLAN Restrictions

■ A port must be a member of at least one VLAN. In the factory default configuration, all ports are assigned to the default VLAN (DEFAULT_VLAN; VID = 1).

■ A port can be a member of one untagged, port-based VLAN. All other port-based VLAN assignments for that port must be tagged. (The “Untagged” designation enables VLAN operation with non 802.1Q-compliant devices.)

■ A port can be an untagged member of one protocol-based VLAN of each protocol type. When assigning a port to multiple, protocol-based VLANs sharing the same type, the port can be an untagged member of only one such VLAN.

■ With routing enabled on the switch, the switch can route traffic between:
  • Multiple, port-based VLANs
  • A port-based VLAN and an IPv4 protocol-based VLAN
  • A port-based VLAN and an IPv6 protocol-based VLAN
  • An IPv4 protocol-based VLAN and an IPv6 protocol VLAN.

Other, routable, protocol-based VLANs must use an external router to move traffic between VLANs. With routing disabled, all routing between VLANs must be through an external router.

■ Before you can delete a VLAN, you must first re-assign all ports in the VLAN to another VLAN.
— This page is intentionally unused. —
Overview

This chapter describes GVRP and how to configure it with the switch’s built-in interfaces, and assumes an understanding of VLANs, which are described in chapter 2.

For general information on how to use the switch’s built-in interfaces, refer to these chapters in the Management and Configuration Guide for your switch:

- Chapter 3, “Using the Menu Interface”
- Chapter 4, “Using the Command Line Interface (CLI)”
- Chapter 5, “Using the HP Web Browser Interface”
- Chapter 6, “Switch Memory and Configuration”
Introduction

GVRP—GARP VLAN Registration Protocol—is an application of the Generic Attribute Registration Protocol—GARP. GVRP is defined in the IEEE 802.1Q standard, and GARP is defined in the IEEE 802.1D-1998 standard.

**Note**

To understand and use GVRP you must have a working knowledge of 802.1Q VLAN tagging. (Refer to chapter 2, “Static Virtual LANs (VLANs)”.)

GVRP uses “GVRP Bridge Protocol Data Units” ("GVRP BPDUs") to “advertise” static VLANs. In this manual, a GVRP BPDU is termed an *advertisement*. Advertisements are sent outbound from ports on a switch to the devices directly connected to those ports.

GVRP enables the Series 5300XL switches to dynamically create 802.1Q-compliant VLANs on links with other devices running GVRP. This enables the switch to automatically create VLAN links between GVRP-aware devices. (A GVRP link can include intermediate devices that are not GVRP-aware.) This operation reduces the chances for errors in VLAN configuration by automatically providing VLAN ID (VID) consistency across the network. That is, you can use GVRP to propagate VLANs to other GVRP-aware devices instead of manually having to set up VLANs across your network. After the switch creates a dynamic VLAN, you can optionally use the CLI `static <vlan-id>`

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view GVRP configuration</td>
<td>n/a</td>
<td>page 3-13</td>
<td>page 3-14</td>
<td>page 3-18</td>
</tr>
<tr>
<td>list static and dynamic VLANs on a GVRP-enabled switch</td>
<td>n/a</td>
<td>—</td>
<td>page 3-16</td>
<td>page 3-18</td>
</tr>
<tr>
<td>enable or disable GVRP</td>
<td>disabled</td>
<td>page 3-13</td>
<td>page 3-15</td>
<td>page 3-18</td>
</tr>
<tr>
<td>enable or disable GVRP on individual ports</td>
<td>enabled</td>
<td>page 3-13</td>
<td>page 3-15</td>
<td>—</td>
</tr>
<tr>
<td>control how individual ports handle advertisements for new VLANs</td>
<td>Learn</td>
<td>page 3-13</td>
<td>page 3-15</td>
<td>page 3-18</td>
</tr>
<tr>
<td>convert a dynamic VLAN to a static VLAN</td>
<td>n/a</td>
<td>—</td>
<td>page 3-17</td>
<td>—</td>
</tr>
<tr>
<td>configure static VLANs</td>
<td>DEFAULT_VLAN (VID = 1)</td>
<td>page 2-21</td>
<td>page 2-27</td>
<td>page 2-37</td>
</tr>
</tbody>
</table>
command to convert it to a static VLAN or allow it to continue as a dynamic VLAN for as long as needed. You can also use GVRP to dynamically enable port membership in static VLANs configured on a switch.

General Operation

When GVRP is enabled on a switch, the VID for any static VLANs configured on the switch is advertised (using BPDUs—Bridge Protocol Data Units) out all ports, regardless of whether a port is up or assigned to any particular VLAN. A GVRP-aware port on another device that receives the advertisements over a link can dynamically join the advertised VLAN.

A dynamic VLAN (that is, a VLAN learned through GVRP) is tagged on the port on which it was learned. Also, a GVRP-enabled port can forward an advertisement for a VLAN it learned about from other ports on the same switch (internal source), but the forwarding port will not itself join that VLAN until an advertisement for that VLAN is received through a link from another device (external source) on that specific port.
Operating Note: When a GVRP-aware port on a switch learns a VID through GVRP from another device, the switch begins advertising that VID out all of its ports except the port on which the VID was learned.

Core switch with static VLANs (VID= 1, 2, & 3). Port 2 is a member of VIDs 1, 2, & 3.

1. Port 2 advertises VIDs 1, 2, & 3.

2. Port 1 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.

3. Port 3 advertises VIDs 1, 2, & 3, but port 3 is NOT a member of VIDs 1, 2, & 3 at this point.

4. Port 4 receives advertisement of VIDs 1, 2, & 3 AND becomes a member of VIDs 1, 2, & 3.

5. Port 5 advertises VIDs 1, 2, & 3, but port 5 is NOT a member of VIDs 1, 2, & 3 at this point.

6. Port 6 is statically configured to be a member of VID 3.

Figure 3-1. Example of Forwarding Advertisements and Dynamic Joining

Note that if a static VLAN is configured on at least one port of a switch, and that port has established a link with another device, then all other ports of that switch will send advertisements for that VLAN.

For example, in the following figure, Tagged VLAN ports on switch “A” and switch “C” advertise VLANs 22 and 33 to ports on other GVRP-enabled switches that can dynamically join the VLANs.
A port can learn of a dynamic VLAN through devices that are not aware of GVRP (Switch “B”, above). VLANs must be disabled in GVRP-unaware devices to allow tagged packets to pass through.

A GVRP-aware port receiving advertisements has these options:

- If there is not already a static VLAN with the advertised VID on the receiving port, then dynamically create the VLAN and become a member.
- If the switch already has a static VLAN assignment with the same VID as in the advertisement, and the port is configured to Auto for that VLAN, then the port will dynamically join the VLAN and begin moving that VLAN’s traffic. (For more detail on Auto, see “Per-Port Options for Dynamic VLAN Advertising and Joining” on page 3-9.)
- Ignore the advertisement for that VID.
- Don’t participate in that VLAN.

Note also that a port belonging to a Tagged or Untagged static VLAN has these configurable options:
Per-Port Options for Handling GVRP “Unknown VLANs”

An “unknown VLAN” is a VLAN that the switch learns of by receiving an advertisement for that VLAN on a port that is not already a member of that VLAN. If the port is configured to learn unknown VLANs, then the VLAN is dynamically created and the port becomes a tagged member of the VLAN. For example, suppose that in figure 3-2 (page 3-6), port 1 on switch “A” is connected to port 5 on switch “C”. Because switch “A” has VLAN 22 statically configured, while switch “C” does not have this VLAN statically configured (and does not “Forbid” VLAN 22 on port 5), VLAN 22 is handled as an “Unknown VLAN” on port 5 in switch “C”. Conversely, if VLAN 22 was statically configured on switch C, but port 5 was not a member, port 5 would become a member when advertisements for VLAN 22 were received from switch “A”.

When you enable GVRP on a switch, you have the per-port join-request options listed in table 3-3-1:
Table 3-1. Options for Handling “Unknown VLAN” Advertisements:

<table>
<thead>
<tr>
<th>Unknown VLAN Mode</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn (the Default)</td>
<td>Enables the port to become a member of any unknown VLAN for which it receives an advertisement. Allows the port to advertise other VLANs that have at least one other port on the same switch as a member.</td>
</tr>
<tr>
<td>Block</td>
<td>Prevents the port from joining any new dynamic VLANs for which it receives an advertisement. Allows the port to advertise other VLANs that have at least one other port as a member.</td>
</tr>
<tr>
<td>Disable</td>
<td>Causes the port to ignore and drop all GVRP advertisements it receives and also prevents the port from sending any GVRP advertisements.</td>
</tr>
</tbody>
</table>

The CLI `show gvrp` command and the menu interface VLAN Support screen show a switch's current GVRP configuration, including the Unknown VLAN settings.

```
HPswitch# show gvrp
GVRP support
Maximum VLANs to support : 8
GVRP Enabled : Yes

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Unknown VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 10/100TX</td>
<td>Learn</td>
</tr>
<tr>
<td>A2 10/100TX</td>
<td>Learn</td>
</tr>
<tr>
<td>A3 10/100TX</td>
<td>Block</td>
</tr>
<tr>
<td>A4 10/100TX</td>
<td>Block</td>
</tr>
<tr>
<td>A5 10/100TX</td>
<td>Learn</td>
</tr>
<tr>
<td>A6 10/100TX</td>
<td>Disable</td>
</tr>
<tr>
<td>A7 10/100TX</td>
<td>Learn</td>
</tr>
<tr>
<td>A8 10/100TX</td>
<td>Learn</td>
</tr>
</tbody>
</table>
```

Figure 3-3. Example of GVRP Unknown VLAN Settings
Per-Port Options for Dynamic VLAN Advertising and Joining

**Initiating Advertisements.** As described in the preceding section, to enable dynamic joins, GVRP must be enabled and a port must be configured to Learn (the default). However, to send advertisements in your network, one or more static (Tagged, Untagged, or Auto) VLANs must be configured on one or more switches (with GVRP enabled), depending on your topology.

**Enabling a Port for Dynamic Joins.** You can configure a port to dynamically join a static VLAN. The join will then occur if that port subsequently receives an advertisement for the static VLAN. (This is done by using the Auto and Learn options described in table 3-3-2, below.

**Parameters for Controlling VLAN Propagation Behavior.** You can configure an individual port to actively or passively participate in dynamic VLAN propagation or to ignore dynamic VLAN (GVRP) operation. These options are controlled by the GVRP “Unknown VLAN” and the static VLAN configuration parameters, as described in the following table:
## Table 3-2. Controlling VLAN Behavior on Ports with Static VLANs

<table>
<thead>
<tr>
<th>Per-Port “Unknown VLAN” (GVRP) Configuration</th>
<th>Static VLAN Options—Per VLAN Specified on Each Port</th>
<th>Port Activity: Tagged or Untagged (Per VLAN)(^2)</th>
<th>Port Activity: Auto(^2) (Per VLAN)</th>
<th>Port Activity: Forbid (Per VLAN)(^2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn (the Default)</td>
<td>The port:</td>
<td>The port:</td>
<td>The port:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Belongs to specified VLAN.</td>
<td>• Will become a member of specified VLAN if it receives advertisements for specified VLAN from another device.</td>
<td>1. Will not become a member of the specified VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advertises specified VLAN.</td>
<td>• Will advertise specified VLAN.</td>
<td>2. Will not advertise specified VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Can become a member of dynamic VLANs for which it receives advertisements.</td>
<td>• Can become a member of other, dynamic VLANs for which it receives advertisements.</td>
<td>3. Can become a member of other dynamic VLANs for which it receives advertisements.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advertises dynamic VLANs that have at least one other port (on the same switch) as a member.</td>
<td>• Will advertise a dynamic VLAN that has at least one other port (on the same switch) as a member.</td>
<td>4. Will advertise a dynamic VLAN that has at least one other port on the same switch as a member.</td>
<td></td>
</tr>
<tr>
<td>Block</td>
<td>The port:</td>
<td>The port:</td>
<td>The port:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Belongs to the specified VLAN.</td>
<td>• Will become a member of specified VLAN if it receives advertisements for this VLAN.</td>
<td>• Will not become a member of this VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Advertises this VLAN.</td>
<td>• Will advertise this VLAN.</td>
<td>• Will ignore GVRP PDUs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will not become a member of new dynamic VLANs for which it receives advertisements.</td>
<td>• Will not become a member of new dynamic VLANs for which it receives advertisements.</td>
<td>• Will not join any advertised VLANs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will advertise dynamic VLANs that have at least one other port as a member.</td>
<td>• Will advertise dynamic VLANs that have at least one other port (on the same switch) as a member.</td>
<td>• Will not advertise VLANs.</td>
<td></td>
</tr>
<tr>
<td>Disable</td>
<td>The port:</td>
<td>The port:</td>
<td>The port:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Is a member of the specified VLAN.</td>
<td>• Will not become a member of the specified VLAN.</td>
<td>• Will not become a member of the specified VLAN.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will ignore GVRP PDUs.</td>
<td>• Will ignore GVRP PDUs.</td>
<td>• Will ignore GVRP PDUs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will not join any advertised VLANs.</td>
<td>• Will not join any dynamic VLANs.</td>
<td>• Will not join any dynamic VLANs.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Will not advertise VLANs.</td>
<td>• Will not advertise VLANs.</td>
<td>• Will not advertise VLANs.</td>
<td></td>
</tr>
</tbody>
</table>

1 Each port of a Series 5300XL switches must be a Tagged or Untagged member of at least one VLAN. Thus, any port configured for GVRP to Learn or Block will generate and forward advertisements for static VLAN(s) configured on the switch and also for dynamic VLANs the switch learns on other ports.

2 To configure tagging, **Auto**, or **Forbid**, see “Configuring Static VLAN Per-Port Settings” on page 2-36 (for the CLI) or “Adding or Changing a VLAN Port Assignment” on page 2-25 (for the menu).
As the preceding table indicates, when you enable GVRP, a port that has a Tagged or Untagged static VLAN has the option for both generating advertisements and dynamically joining other VLANs.

**Note**

In table 3-3-2, above, the Unknown VLAN parameters are configured on a per-port basis using the CLI. The Tagged, Untagged, Auto, and Forbid options are configured per static VLAN on every port, using either the menu interface or the CLI.

Because dynamic VLANs operate as Tagged VLANs, and because a tagged port on one device cannot communicate with an untagged port on another device, HP recommends that you use Tagged VLANs for the static VLANs you will use to generate advertisements.

## GVRP and VLAN Access Control

When you enable GVRP on a switch, the default GVRP parameter settings allow all of the switch’s ports to transmit and receive dynamic VLAN advertisements (GVRP advertisements) and to dynamically join VLANs. The two preceding sections describe the per-port features you can use to control and limit VLAN propagation. To summarize, you can:

- Allow a port to advertise and/or join dynamic VLANs (Learn mode—the default).
- Allow a port to send VLAN advertisements, but not receive them from other devices; that is, the port cannot dynamically join a VLAN but other devices can dynamically join the VLANs it advertises (Block mode).
- Prevent a port from participating in GVRP operation (Disable mode).

## Port-Leave From a Dynamic VLAN

A dynamic VLAN continues to exist on a port for as long as the port continues to receive advertisements of that VLAN from another device connected to that port or until you:

- Convert the VLAN to a static VLAN (See “Converting a Dynamic VLAN to a Static VLAN” on page 3-17.)
- Reconfigure the port to **Block** or **Disable**
- Disable GVRP
- Reboot the switch
The time-to-live for dynamic VLANs is 10 seconds. That is, if a port has not received an advertisement for an existing dynamic VLAN during the last 10 seconds, the port removes itself from that dynamic VLAN.

Planning for GVRP Operation

These steps outline the procedure for setting up dynamic VLANs for a segment.

1. Determine the VLAN topology you want for each segment (broadcast domain) on your network.

2. Determine the VLANs that must be static and the VLANs that can be dynamically propagated.

3. Determine the device or devices on which you must manually create static VLANs in order to propagate VLANs throughout the segment.

4. Determine security boundaries and how the individual ports in the segment will handle dynamic VLAN advertisements. (See table 3-3-1 on page 3-8 and table 3-3-2 on page 3-10.)

5. Enable GVRP on all devices you want to use with dynamic VLANs and configure the appropriate “Unknown VLAN” parameter (Learn, Block, or Disable) for each port.

6. Configure the static VLANs on the switch(es) where they are needed, along with the per-VLAN parameters (Tagged, Untagged, Auto, and Forbid—see table 3-3-2 on page 3-10) on each port.

7. Dynamic VLANs will then appear automatically, according to the configuration options you have chosen.

8. Convert dynamic VLANs to static VLANs where you want dynamic VLANs to become permanent.
Configuring GVRP On a Switch

The procedures in this section describe how to:

- View the GVRP configuration on a switch
- Enable and disable GVRP on a switch
- Specify how individual ports will handle advertisements

To view or configure static VLANs for GVRP operation, refer to “Per-Port Static VLAN Configuration Options” on page 2-11.

Menu: Viewing and Configuring GVRP

1. From the Main Menu, select:
   
   **2. Switch Configuration …**
   
   **8. VLAN Menu …**
   
   **1. VLAN Support**

   ![VLAN Support Screen](image)

   **Figure 3-4. The VLAN Support Screen (Default Configuration)**

2. Do the following to enable GVRP and display the Unknown VLAN fields:
   
   a. Press **E** (for **Edit**).
   b. Use **↓** to move the cursor to the **GVRP Enabled** field.
   c. Press the Space bar to select **Yes**.
   d. Press **↓** again to display the **Unknown VLAN** fields.
The Unknown VLAN fields enable you to configure each port to:
- Learn - Dynamically join any advertised VLAN and advertise all VLANs learned through other ports.
- Block - Do not dynamically join any VLAN, but still advertise all VLANs learned through other ports.
- Disable - Ignore and drop all incoming advertisements and do not transmit any advertisements.

Figure 3-5. Example Showing Default Settings for Handling Advertisements

3. Use the arrow keys to select the port you want, and the Space bar to select Unknown VLAN option for any ports you want to change.

4. When you finish making configuration changes, press [Enter], then [S] (for Save) to save your changes to the Startup-Config file.

CLI: Viewing and Configuring GVRP

GVRP Commands Used in This Section

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show gvrp below</td>
<td>3-15</td>
</tr>
<tr>
<td>gvrp</td>
<td>3-15</td>
</tr>
<tr>
<td>unknown-vlans</td>
<td>3-15</td>
</tr>
</tbody>
</table>

Displaying the Switch’s Current GVRP Configuration. This command shows whether GVRP is disabled, along with the current settings for the maximum number of VLANs and the current Primary VLAN. (For more on the last two parameters, see chapter 2, “Static Virtual LANs (VLANs)”.)

Syntax: show gvrp

Shows the current settings.
Figure 3-6. Example of “Show GVRP” Listing with GVRP Disabled

```
HPswitch> show gvrp
GVRP support
  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : No
```

Figure 3-7. Example of Show GVRP Listing with GVRP Enabled

```
HPswitch> show gvrp
GVRP support
  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : Yes

Port Type | Unknown VLAN
---------|--------------
A1  10/100TX | Learn
A2  10/100TX | Learn
A3  10/100TX | Block
A4  10/100TX | Disable
A5  10/100TX | Disable
A6  10/100TX | Learn
A7  10/100TX | Learn
  .  .  .  .
  .  .  .  .

This example includes non-default settings for the Unknown VLAN field for some ports.
```

Enabling and Disabling GVRP on the Switch. This command enables GVRP on the switch.

**Syntax:**

```
gvrp
```

This example enables GVRP:

```
HPswitch(config)# gvrp
```

This example disables GVRP operation on the switch:

```
HPswitch(config)# no gvrp
```

Enabling and Disabling GVRP On Individual Ports. When GVRP is enabled on the switch, use the `unknown-vlans` command to change the Unknown VLAN field for one or more ports. You can use this command at either the Manager level or the interface context level for the desired port(s).
Syntax: interface <port-list> unknown-vlans <learn | block | disable>

Changes the Unknown VLAN field setting for the specified port(s).

For example, to change and view the configuration for ports A1-A2 to Block:

```
HPswitch(config)#interface a1-a2 unknown-vlans block
```

```
HP4106(config)#show gvrp
GVRP support
  Maximum VLANs to support : 8
  Primary VLAN : DEFAULT_VLAN
  GVRP Enabled : Yes

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Unknown VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 10/100TX</td>
<td>Block</td>
</tr>
<tr>
<td>2 10/100TX</td>
<td>Block</td>
</tr>
<tr>
<td>3 10/100TX</td>
<td>Learn</td>
</tr>
<tr>
<td>4 10/100TX</td>
<td>Learn</td>
</tr>
</tbody>
</table>
```

Figure 3-8. Displaying the Static and Dynamic VLANs Active on the Switch

Syntax: show vlans

The show vlans command lists all VLANs present in the switch.

For example, in the following illustration, switch “B” has one static VLAN (the default VLAN), with GVRP enabled and port 1 configured to Learn for Unknown VLANs. Switch “A” has GVRP enabled and has three static VLANs: the default VLAN, VLAN-222, and VLAN-333. In this scenario, switch B will dynamically join VLAN-222 and VLAN-333:
The `show vlans` command lists the dynamic (and static) VLANs in switch “B” after it has learned and joined VLAN-222 and VLAN-333.

![Figure 3-9. Example of Listing Showing Dynamic VLANs](image)

**Converting a Dynamic VLAN to a Static VLAN.** If a port on the switch has joined a dynamic VLAN, you can use the following command to convert that dynamic VLAN to a static VLAN:

**Syntax:**

```
static < dynamic-vlan-id >
```

*Converts the a dynamic VLAN to a static VLAN.*

For example, to convert dynamic VLAN 333 (from the previous example) to a static VLAN:

```
HPswitch(config)# static 333
```

When you convert a dynamic VLAN to a static VLAN, all ports on the switch are assigned to the VLAN in Auto mode.
Web: Viewing and Configuring GVRP

To view, enable, disable, or reconfigure GVRP:

1. Click on the **Configuration** tab.

2. Click on [VLAN Configuration] and do the following:
   - To enable or disable GVRP, click on **GVRP Enabled**.
   - To change the Unknown VLAN field for any port:
     i. Click on [GVRP Security] and make the desired changes.
     ii. Click on [Apply] to save and implement your changes to the Unknown VLAN fields.

For web-based Help on how to use the web browser interface screen, click on the [?] button provided on the web browser screen.

---

GVRP Operating Notes

- A dynamic VLAN must be converted to a static VLAN before it can have an IP address.

- The total number of VLANs on the switch (static and dynamic combined) cannot exceed the current Maximum VLANs setting. For example, in the factory default state, the switch supports eight VLANs. Thus, in a case where four static VLANs are configured on the switch, the switch can accept up to four additional VLANs in any combination of static and dynamic. Any additional VLANs advertised to the switch will not be added unless you first increase the Maximum VLANs setting. In the Menu interface, click on **2. Switch Configuration … 8. VLAN Menu 1. VLAN Support**. In the global config level of the CLI, use `max-vlans`.

- Converting a dynamic VLAN to a static VLAN and then executing the **write memory** command saves the VLAN in the startup-config file and makes it a permanent part of the switch’s VLAN configuration.

- Within the same broadcast domain, a dynamic VLAN can pass through a device that is not GVRP-aware. This is because a hub or a switch that is not GVRP-aware will flood the GVRP (multicast) advertisement packets out all ports.

- GVRP assigns dynamic VLANs as Tagged VLANs. To configure the VLAN as Untagged, you must first convert it to a static VLAN.
- Rebooting a switch on which a dynamic VLAN exists deletes that VLAN. However, the dynamic VLAN re-appears after the reboot if GVRP is enabled and the switch again receives advertisements for that VLAN through a port configured to add dynamic VLANs.

- By receiving advertisements from other devices running GVRP, the switch learns of static VLANs on those other devices and dynamically (automatically) creates tagged VLANs on the links to the advertising devices. Similarly, the switch advertises its static VLANs to other GVRP-aware devices, as well as the dynamic VLANs the switch has learned.

- A GVRP-enabled switch does not advertise any GVRP-learned VLANs out of the port(s) on which it originally learned of those VLANs.
This page intentionally unused.
Multimedia Traffic Control with IP Multicast (IGMP)

Contents

Overview ................................................................. 4-2
IGMP General Operation and Features ................................. 4-3
  IGMP Terms ....................................................... 4-4
  IGMP Operating Features ........................................ 4-5
    Basic Operation ............................................... 4-5
    Enhancements ................................................ 4-5
CLI: Configuring and Displaying IGMP ................................. 4-6
Web: Enabling or Disabling IGMP .................................... 4-11
How IGMP Operates .................................................... 4-11
  Operation With or Without IP Addressing ........................ 4-13
  Automatic Fast-Leave IGMP ...................................... 4-13
  Forced Fast-Leave IGMP ......................................... 4-15
    Configuration Options for Forced Fast-Leave ................ 4-15
    Listing the Forced Fast-Leave Configuration ................ 4-16
    Configuring Per-Port Forced Fast-Leave IGMP ............... 4-18
Using the Switch as Querier .......................................... 4-19
Excluding Well-Known or Reserved Multicast Addresses from IP Multicast Filtering ............................. 4-20
  IP Multicast Filters ............................................. 4-21
  Reserved Addresses Excluded from IP Multicast (IGMP) Filtering ...................................................... 4-21
  Number of IP Multicast Addresses Allowed ..................... 4-21
Overview

This chapter describes multimedia traffic control with IP multicast (IGMP) to reduce unnecessary bandwidth usage on a per-port basis, and how to configure it with the switch’s built-in interfaces:

For general information on how to use the switch’s built-in interfaces, refer to these chapters in the Management and Configuration Guide for your switch:

- Chapter 3, “Using the Menu Interface”
- Chapter 4, “Using the Command Line Interface (CLI)”
- Chapter 5, “Using the HP Web Browser Interface”
- Chapter 6, “Switch Memory and Configuration”
IGMP General Operation and Features

### IGMP Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>view igmp configuration</td>
<td>n/a</td>
<td>—</td>
<td>page 4-6</td>
<td>—</td>
</tr>
<tr>
<td>show igmp status for multicast groups used by the selected VLAN</td>
<td>n/a</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>enabling or disabling IGMP (Requires VLAN ID Context)</td>
<td>disabled</td>
<td>—</td>
<td>page 4-8</td>
<td>page 4-11</td>
</tr>
<tr>
<td>per-port packet control</td>
<td>auto</td>
<td>—</td>
<td>page 4-9</td>
<td>—</td>
</tr>
<tr>
<td>IGMP traffic priority</td>
<td>normal</td>
<td>—</td>
<td>page 4-10</td>
<td>—</td>
</tr>
<tr>
<td>querier</td>
<td>enabled</td>
<td>—</td>
<td>page 4-10</td>
<td>—</td>
</tr>
<tr>
<td>fast-leave</td>
<td>disabled</td>
<td>—</td>
<td>page 4-13</td>
<td>—</td>
</tr>
</tbody>
</table>

In a network where IP multicast traffic is transmitted for various multimedia applications, you can use the switch to reduce unnecessary bandwidth usage on a per-port basis by configuring IGMP (Internet Group Management Protocol controls). In the factory default state (IGMP disabled), the switch simply floods all IP multicast traffic it receives on a given VLAN through all ports on that VLAN (except the port on which it received the traffic). This can result in significant and unnecessary bandwidth usage in networks where IP multicast traffic is a factor. Enabling IGMP allows the ports to detect IGMP queries and report packets and manage IP multicast traffic through the switch.

IGMP is useful in multimedia applications such as LAN TV, desktop conferencing, and collaborative computing, where there is multipoint communication; that is, communication from one to many hosts, or communication originating from many hosts and destined for many other hosts. In such multipoint applications, IGMP will be configured on the hosts, and multicast traffic will be generated by one or more servers (inside or outside of the local network). Switches in the network (that support IGMP) can then be configured to direct the multicast traffic to only the ports where needed. If multiple VLANs are configured, you can configure IGMP on a per-VLAN basis.
Enabling IGMP allows detection of IGMP queries and report packets in order to manage IP multicast traffic through the switch. If no other querier is detected, the switch will then also function as the querier. (If you need to disable the querier feature, you can do so through the IGMP configuration MIB. Refer to “Changing the Querier Configuration Setting” on page 4-10.)

**Note**

IGMP configuration on the Series 5300XL switches operates at the VLAN context level. If you are not using VLANs, then configure IGMP in VLAN 1 (the default VLAN) context.

**IGMP Terms**

- **IGMP Device**: A switch or router running IGMP traffic control features.

- **IGMP Host**: An end-node device running an IGMP (multipoint, or multicast communication) application.

- **Querier**: A required IGMP device that facilitates the IGMP protocol and traffic flow on a given LAN. This device tracks which ports are connected to devices (IGMP clients) that belong to specific multicast groups, and triggers updates of this information. A querier uses data received from the queries to determine whether to forward or block multicast traffic on specific ports. When the switch has an IP address on a given VLAN, it automatically operates as a Querier for that VLAN if it does not detect a multicast router or another switch functioning as a Querier. When enabled (the default state), the switch’s querier function eliminates the need for a multicast router. In most cases, HP recommends that you leave this parameter in the default “enabled” state even if you have a multicast router performing the querier function in your multicast group. For more information, see “How IGMP Operates” on page 4-11.
IGMP Operating Features

Basic Operation

In the factory default configuration, IGMP is disabled. To enable IGMP

- If multiple VLANs are not configured, you configure IGMP on the default VLAN (DEFAULT_VLAN; VID = 1).
- If multiple VLANs are configured, you configure IGMP on a per-VLAN basis for every VLAN where this feature is to be used.

Enhancements

With the CLI, you can configure these additional options:

- **Forward with High Priority:** Disabling this parameter (the default) causes the switch or VLAN to process IP multicast traffic, along with other traffic, in the order received (usually, normal priority). Enabling this parameter causes the switch or VLAN to give a higher priority to IP multicast traffic than to other traffic.

- **Auto/Blocked/Forward:** You can use the console to configure individual ports to any of the following states:
  - **Auto** (the default): Causes the switch to interpret IGMP packets and to filter IP multicast traffic based on the IGMP packet information for ports belonging to a multicast group. This means that IGMP traffic will be forwarded on a specific port only if an IGMP host or multicast router is connected to the port.
  - **Blocked:** Causes the switch to drop all IGMP transmissions received from a specific port and to block all outgoing IP Multicast packets for that port. This has the effect of preventing IGMP traffic from moving through specific ports.
  - **Forward:** Causes the switch to forward all IGMP and IP multicast transmissions through the port.

- **Operation With or Without IP Addressing:** This feature helps to conserve IP addresses by enabling IGMP to run on VLANs that do not have an IP address. See “Operation With or Without IP Addressing” on page 4-13.

- **Querier Capability:** The switch performs this function for IGMP on VLANs having an IP address when there is no other device in the VLAN acting as querier. See “Using the Switch as Querier” on page 4-19.
Notes

Whenever IGMP is enabled, the switch generates an Event Log message indicating whether querier functionality is enabled.

IP multicast traffic groups are identified by IP addresses in the range of 224.0.0.0 to 239.255.255.255. Also, incoming IGMP packets intended for reserved, or “well-known” multicast addresses automatically flood through all ports (except the port on which the packets entered the switch). For more on this topic, see “Excluding Well-Known or Reserved Multicast Addresses from IP Multicast Filtering” on page 4-20.

For more information, refer to “How IGMP Operates” on page 4-11.

CLI: Configuring and Displaying IGMP

IGMP Commands Used in This Section

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp configuration</td>
<td>4-7</td>
</tr>
<tr>
<td>ip igmp</td>
<td>4-8</td>
</tr>
<tr>
<td>high-priority-forward</td>
<td>4-10</td>
</tr>
<tr>
<td>auto &lt;[ethernet] &lt;port-list&gt;</td>
<td>4-9</td>
</tr>
<tr>
<td>blocked &lt;[ethernet] &lt;port-list&gt;</td>
<td>4-9</td>
</tr>
<tr>
<td>forward &lt;[ethernet] &lt;port-list&gt;</td>
<td>4-9</td>
</tr>
<tr>
<td>querier</td>
<td>4-10</td>
</tr>
<tr>
<td>show ip igmp</td>
<td></td>
</tr>
</tbody>
</table>

Refer to the section titled “Internet Group Management Protocol (IGMP) Status” in appendix B of the Management and Configuration Guide for your switch.
Viewing the Current IGMP Configuration. This command lists the IGMP configuration for all VLANs configured on the switch or for a specific VLAN.

Syntax: show ip igmp config

Displays IGMP configuration for all VLANs on the switch.

show ip igmp vlan < vid > config

Displays IGMP configuration for a specific VLAN on the switch, including per-port data.

(For IGMP operating status, refer to the section titled “Internet Group Management Protocol (IGMP) Status” in appendix B, “Monitoring and Analyzing Switch Operation” of the Management and Configuration Guide for your switch.)

For example, suppose you have the following VLAN and IGMP configurations on the switch:

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>IGMP Enabled</th>
<th>Forward with High Priority</th>
<th>Querier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>22</td>
<td>VLAN-2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>33</td>
<td>VLAN-3</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

You could use the CLI to display this data as follows:

```
HPswitch> show ip igmp config
IGMP Service

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN NAME</th>
<th>IGMP Enabled</th>
<th>Forward with High Priority</th>
<th>Querier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>22</td>
<td>VLAN-2</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>33</td>
<td>VLAN-3</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

Figure 4-1. Example Listing of IGMP Configuration for All VLANs in the Switch
The following version of the `show ip igmp` command includes the VLAN ID (`vid`) designation, and combines the above data with the IGMP per-port configuration:

```
HPswitch(config)# show ip igmp vlan 1 config
IGMP Service
VLAN ID : 1
VLAN NAME : DEFAULT_VLAN
IGMP Enabled : Yes
Forward with High Priority : No
Querier Allowed : Yes

Port Type | IP Mcast
----------+----------
A1 100/1000T | Auto
A2 100/1000T | Auto
A3 100/1000T | Forward
A4 100/1000T | Forward
A5 100/1000T | Blocked
A6 100/1000T | Blocked
```

Figure 4-2. Example Listing of IGMP Configuration for A Specific VLAN

**Enabling or Disabling IGMP on a VLAN.** You can enable IGMP on a VLAN, along with the last-saved or default IGMP configuration (whichever was most recently set), or you can disable IGMP on a selected VLAN.

**Syntax:** `[no] ip igmp

Enables IGMP on a VLAN. Note that this command must be executed in a VLAN context.

For example, here are methods to enable and disable IGMP on the default VLAN (VID = 1).

```
HPswitch(config)# vlan 1 ip igmp

Enables IGMP on VLAN 1.

HPswitch(vlan-1)# ip igmp

Same as above.

HPswitch(config)# no vlan 1 ip igmp

Disables IGMP on vlan 1.
```
If you disable IGMP on a VLAN and then later re-enable IGMP on that VLAN, the switch restores the last-saved IGMP configuration for that VLAN. For more on how switch memory operates, refer to the chapter titled “Switch Memory and Configuration” in the *Management and Configuration Guide* for your switch.

You can also combine the `ip igmp` command with other IGMP-related commands, as described in the following sections.

**Configuring Per-Port IGMP Packet Control.**

**Syntax:** `vlan < vid > ip igmp [auto < port-list > | blocked < port-list > | forward < port-list >]`

*Used in the VLAN context, this command specifies how each port should handle IGMP traffic. (Default: auto.)*

For example, suppose you wanted to configure IGMP as follows for VLAN 1 on the 100/1000T ports on a module in slot 1:

<table>
<thead>
<tr>
<th>Ports</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1-A2</td>
<td>auto</td>
<td>Filter multicast traffic. Forward IGMP traffic to hosts on these ports that belong to the multicast group for which the traffic is intended. (Also forward any multicast traffic through any of these ports that is connected to a multicast router.)</td>
</tr>
<tr>
<td>A3-A4</td>
<td>forward</td>
<td>Forward all multicast traffic through this port.</td>
</tr>
<tr>
<td>A5-A6</td>
<td>blocked</td>
<td>Drop all multicast traffic received from devices on these ports, and prevent any outgoing multicast traffic from moving through these ports.</td>
</tr>
</tbody>
</table>

Depending on the privilege level, you could use one of the following commands to configure IGMP on VLAN 1 with the above settings:

```
HPswitch(config)# vlan 1 ip igmp auto a1,a2 forward a3,a4 blocked a5,a6
```

```
HPswitch(config)# ip igmp auto a1,a2 forward a3,a4 blocked a5,a6
```

The following command displays the VLAN and per-port configuration resulting from the above commands:

```
HPswitch> show igmp vlan 1 config
```
Configuring IGMP Traffic Priority.

**Syntax:** `vlan <vid> ip igmp high-priority-forward`

_This command assigns “high” priority to IGMP traffic or returns a high-priority setting to “normal” priority. (The traffic will be serviced at its inbound priority.) (Default: normal.)_

HPswitch(config)# vlan 1 ip igmp high-priority-forward

_Configures high priority for IGMP traffic on VLAN 1.

HPswitch(vlan-1)# ip igmp high-priority-forward

_Same as above command, but in the VLAN 1 context level.

HPswitch(vlan 1)# no ip igmp high-priority-forward

_Returns IGMP traffic to “normal” priority.

HPswitch> show ip igmp config

_Show command to display results of above high-priority commands.

Configuring the Querier Function.

**Syntax:** `[no] vlan <vid> ip igmp querier`

_This command disables or re-enables the ability for the switch to become querier if necessary. (Default Querier Capability: Enabled.)_

HPswitch(config)# no vlan 1 ip igmp querier

_Disables the querier function on VLAN 1.

HPswitch> show ip igmp config

_Show command to display results of above querier command.
Web: Enabling or Disabling IGMP

In the web browser interface you can enable or disable IGMP on a per-VLAN basis. To configure other IGMP features, telnet to the switch console and use the CLI.

To Enable or Disable IGMP

1. Click on the **Configuration** tab.
2. Click on the **Device Features** button.
3. If more than one VLAN is configured, use the VLAN pull-down menu to select the VLAN on which you want to enable or disable IGMP.
4. Use the Multicast Filtering (IGMP) menu to enable or disable IGMP.
5. Click on **Apply Changes** button to implement the configuration change.

For web-based help on how to use the web browser interface screen, click on the [?] button provided on the web browser screen.

How IGMP Operates

The Internet Group Management Protocol (IGMP) is an internal protocol of the Internet Protocol (IP) suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP. (In Hewlett-Packard's implementation of IGMP, a multicast router is not necessary as long as a switch is configured to support IGMP with the querier feature enabled.) A set of hosts, routers, and/or switches that send or receive multicast data streams to or from the same source(s) is termed a *multicast group*, and all devices in the group use the same multicast group address. The multicast group running version 2 of IGMP uses three fundamental types of messages to communicate:

- **Query**: A message sent from the querier (multicast router or switch) asking for a response from each host belonging to the multicast group. If a multicast router supporting IGMP is not present, then the switch must assume this function in order to elicit group membership information from the hosts on the network. (If you need to disable the querier feature, you can do so through the CLI, using the IGMP configuration MIB. See “Configuring the Querier Function” on page 4-10.)
Multimedia Traffic Control with IP Multicast (IGMP)
How IGMP Operates

- **Report (Join):** A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.

- **Leave Group:** A message sent by a host to the querier to indicate that the host has ceased to be a member of a specific multicast group.

**Note on IGMP version 3 support**

When an IGMPv3 Join is received by the switch, it accepts the host request and begins to forward the IGMP traffic. This means that ports which have not joined the group and are not connected to routers or the IGMP Querier will not receive the group’s multicast traffic.

The switch does not support the IGMPv3 “Exclude Source” or “Include Source” options in the Join Reports. Rather, the group is simply joined from all sources.

The switch does not support becoming a version 3 Querier. It will become a version 2 Querier in the absence of any other Querier on the network.

An IP multicast packet includes the multicast group (address) to which the packet belongs. When an IGMP client connected to a switch port needs to receive multicast traffic from a specific group, it joins the group by sending an IGMP report (join request) to the network. (The multicast group specified in the join request is determined by the requesting application running on the IGMP client.) When a networking device with IGMP enabled receives the join request for a specific group, it forwards any IP multicast traffic it receives for that group through the port on which the join request was received. When the client is ready to leave the multicast group, it sends a Leave Group message to the network and ceases to be a group member. When the leave request is detected, the appropriate IGMP device will cease transmitting traffic for the designated multicast group through the port on which the leave request was received (as long as there are no other current members of that group on the affected port).

Thus, IGMP identifies members of a multicast group (within a subnet) and allows IGMP-configured hosts (and routers) to join or leave multicast groups.

**IGMP Data.** To display data showing active group addresses, reports, queries, querier access port, and active group address data (port, type, and access), refer to the section titled “Internet Group Management Protocol (IGMP) Status” in appendix B, “Monitoring and Analyzing Switch Operation” of the Management and Configuration Guide for your switch.)
Operation With or Without IP Addressing

You can configure IGMP on VLANs that do not have IP addressing. The benefit of IGMP without IP addressing is a reduction in the number of IP addresses you have to use and configure. This can be significant in a network with a large number of VLANs. The limitation on IGMP without IP addressing is that the switch cannot become Querier on any VLANs for which it has no IP address—so the network administrator must ensure that another IGMP device will act as Querier. It is also advisable to have an additional IGMP device available as a backup Querier. See the following table.

Table 4-1. Comparison of IGMP Operation With and Without IP Addressing

<table>
<thead>
<tr>
<th>IGMP Function</th>
<th>Available With IP Addressing Configured on the VLAN</th>
<th>Available Without IP Addressing?</th>
<th>Operating Differences Without an IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward multicast group traffic to any port on the VLAN that has received a join request for that multicast group.</td>
<td>Yes</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Forward join requests (reports) to the Querier.</td>
<td>Yes</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Configure individual ports in the VLAN to Auto (the default)/Blocked, or Forward.</td>
<td>Yes</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Configure IGMP traffic forwarding to normal or high-priority forwarding.</td>
<td>Yes</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Age-Out IGMP group addresses when the last IGMP client on a port in the VLAN leaves the group.</td>
<td>Yes</td>
<td>Requires that another IGMP device in the VLAN has an IP address and can operate as Querier. This can be a multicast router or another switch configured for IGMP operation. (HP recommends that the VLAN also include a device operating as a backup Querier in case the device operating as the primary Querier fails for any reason.</td>
<td></td>
</tr>
<tr>
<td>Support Fast-Leave IGMP and Forced Fast-Leave IGMP (below).</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support automatic Querier election.</td>
<td>No</td>
<td>Querier operation not available.</td>
<td></td>
</tr>
<tr>
<td>Operate as the Querier.</td>
<td>No</td>
<td>Querier operation not available.</td>
<td></td>
</tr>
<tr>
<td>Available as a backup Querier.</td>
<td>No</td>
<td>Querier operation not available.</td>
<td></td>
</tr>
</tbody>
</table>

Automatic Fast-Leave IGMP

**IGMP Operation Presents a “Delayed Leave” Problem.** Where multiple IGMP clients are connected to the same port on an IGMP device (switch or router), if only one IGMP client joins a given multicast group, then later sends a Leave Group message and ceases to belong to that group, the IGMP device retains that IGMP client in its IGMP table and continues forwarding IGMP traffic to the IGMP client until the Querier triggers confirmation that no other
group members exist on the same port. This delayed leave operation means that the switch continues to transmit unnecessary multicast traffic through the port until the Querier renews multicast group status.

**Fast-Leave IGMP Reduces Leave Delays.** Fast-Leave IGMP operates on a port if an IGMP client connects to the port and there are no other end nodes detected on that port. In this case, when the client leaves a multicast group, Fast-Leave IGMP automatically accelerates the blocking of further, unnecessary multicast traffic from that group to the former IGMP client. This improves performance by reducing the amount of multicast traffic going through the port to the IGMP client after the client leaves a multicast group. IGMP in the Series 5300XL switches automatically uses this Fast-Leave feature.

**Automatic Fast-Leave Operation.** If a switch port has the following characteristics, then the Fast-Leave operation will apply:

1. Connected to only one end node
2. The end node currently belongs to a multicast group; i.e. is an IGMP client
3. The end node subsequently leaves the multicast group

Then the switch does not need to wait for the Querier status update interval, but instead immediately removes the IGMP client from its IGMP table and ceases transmitting IGMP traffic to the client. (If the switch detects multiple end nodes on the port, automatic Fast-Leave does not activate—regardless of whether one or more of these end nodes are IGMP clients.)

In the next figure, automatic Fast-Leave operates on the switch ports for IGMP clients “3A” and “5A”, but not on the switch port for IGMP clients “7A” and 7B, Server “7C”, and printer “7D”.

![Figure 4-3. Example of Automatic Fast-Leave IGMP Criteria](image_url)

When client “3A” running IGMP is ready to leave the multicast group, it transmits a Leave Group message. Because the switch knows that there is only one end node on port A3, it removes the client from its IGMP table and halts...
Multimedia Traffic Control with IP Multicast (IGMP)

How IGMP Operates

Multicast traffic (for that group) to port A3. If the switch is not the Querier, it does not wait for the actual Querier to verify that there are no other group members on port A3. If the switch itself is the Querier, it does not query port A3 for the presence of other group members.

Note that Fast-Leave operation does not distinguish between end nodes on the same port that belong to different VLANs. Thus, for example, even if all of the devices on port A6 in figure 4-3 belong to different VLANs, Fast-Leave does not operate on port A6.

Forced Fast-Leave IGMP

Forced Fast-Leave IGMP speeds up the process of blocking unnecessary IGMP traffic to a switch port that is connected to multiple end nodes. (This feature does not activate on ports where the switch detects only one end node). For example, in figure 4-3, even if you configured Forced Fast-Leave on all ports in the switch, the feature would activate only on port A6 (which has multiple end nodes) when a Leave Group request arrived on that port.

When a port having multiple end nodes receives a Leave Group request from one end node for a given multicast group “X”, Forced Fast-Leave activates and waits a small amount of time to receive a join request from any other group “X” member on that port. If the port does not receive a join request for that group within the forced-leave interval, the switch then blocks any further group “X” traffic to the port.

Configuration Options for Forced Fast-Leave

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Settings</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forced Fast-Leave state</td>
<td>2 (disabled)</td>
<td>1 (enabled) 2 (disabled)</td>
<td>Uses the setmib command to enable or disable Forced Fast-Leave on individual ports. When enabled on a port, Forced Fast-Leave operates only if the switch detects multiple end nodes (and at least one IGMP client) on that port.</td>
</tr>
</tbody>
</table>

Note on VLAN Numbers

In the HP Procurve Series 5300XL switch, the walkmib and setmib commands use an internal VLAN number (and not the VLAN ID, or VID) to display or change many per-vlan features, such as the Forced Fast-Leave state. Because the internal VLAN number for the default VLAN is always 1 (regardless of whether VLANs are enabled on the switch), and because a discussion of internal VLAN numbers for multiple VLANs is beyond the scope of this document, the discussion here concentrates on examples that use the default VLAN.
Listing the Forced Fast-Leave Configuration

The Forced Fast-Leave configuration data is available in the switch’s MIB (Management Information Base), and includes the state (enabled or disabled) for each port and the Forced-Leave Interval for all ports on the switch.

Note on Port Numbers

For the IGMP MIB commands that are described on the next few pages, the HP Procurve Switch 5300xl uses 26 ports for each slot. This is true regardless of the type of modules that you have installed in the slots. The following port numbering is used:

- Slot A = ports 1-24 (ports 25 and 26 are reserved)
- Slot B = ports 27-50 (ports 51 and 52 are reserved)

To List the Forced Fast-Leave State for all Ports in the Switch. Go to the switch’s command prompt and use the walkmib command, as shown below.

1. From the Main Menu, select:
   5. Diagnostics . . .
   4. Command Prompt

2. Do one of the following:
   - If VLANs are not enabled on the switch, go to step 3.
   - If VLANs are enabled on the switch:
     i. You will be prompted to select a VLAN. For example:

   Select VLAN : DEFAULT VLAN

     ii. Because you can list the Forced Fast-Leave state for all ports on the switch from any VLAN, just press [Enter] to select the displayed VLAN.

3. Enter either of the following walkmib command options:

   walkmib hpSwitchIgmpPortForcedLeaveState

   - OR -

   walkmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5

   The resulting display lists the Forced Fast-Leave state for all ports in the switch, by VLAN. (A port belonging to more than one VLAN will be listed once for each VLAN, and if multiple VLANs are not configured, all ports will be listed as members of the default VLAN.) The following command produces a listing such as that shown in figure 4-4:
How IGMP Operates

The \( 1 \) at the end of a port listing shows that Forced Fast-Leave is enabled on the corresponding port.

The \( 2 \) at the end of a port listing shows that Forced Fast-Leave is disabled on the corresponding port.

**Ports 1-6: 6- Port 109/1000T Module in Slot A**

**Figure 4-4. Example of a Forced Fast-Leave Listing where all Ports are Members of the Default VLAN**

To List the Forced Fast-Leave State for a Single Port. (See the “Note on VLAN Numbers” on page 4-15.)

Use the switch’s CLI and use the `getmib` command, as shown below.

**Syntax:**

```
getmib hpSwitchIgmpPortForcedLeaveState.<vlan number> | .port number >
```

- OR -

```
getmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5.<vlan number> | .port number >
```

For example, the following command to list the state for port A6 (which, in this case, belongs to the default VLAN) produces the indicated listing:

**Figure 4-5. Example Listing the Forced Fast-Leave State for a Single Port on the Default VLAN**

```bash
HPswitch(config)# getmib hpSwitchIgmpPortForcedLeaveState.1.6
hpSwitchIgmpPortForcedLeaveState.1.6 = 2
```
Configuring Per-Port Forced Fast-Leave IGMP

In the factory-default configuration, Forced Fast-Leave is disabled for all ports on the switch. To enable (or disable) this feature on individual ports, use the switch’s `setmib` command, as shown below.

**Configuring Per-Port Forced Fast-Leave IGMP on Ports.**

**Syntax:**

```
setmib hpSwitchIgmpPortForcedLeaveState.<vid>.<port-nmbr> -i <1 | 2>
```

OR

```
setmib 1.3.6.1.4.1.11.2.14.11.5.1.7.1.15.3.1.5.<vid>.<port-nmbr> -i <1 | 2>
```

*where:*

1 = Forced Fast-Leave enabled
2 = Forced Fast-Leave disabled

*This procedure enables or disables Forced Fast-Leave on ports in a given VLAN. (See the “Note on VLAN Numbers” on page 4-15.)*

For example, suppose that your switch has a six-port gigabit module in slot A, and port C1 is a member of the default VLAN. In this case, the port number is “53” (In the MIB, slot A = ports 1-24; slot B = ports 27-50; slot C = ports 53-79, and so on.) To enable Forced Fast-Leave on C1 (53), you would execute the following command and see the indicated result:

```
DEFAULT_CONFIG: setmib hpSwitchIgmpPortForcedLeaveState.1.53 -i
```

```
HPswitch(config)# setmib hpSwitchIgmpPortForcedLeaveState.1.49 -i 1
hpSwitchIgmpPortForcedLeaveState.1.49 = 1
```

Verifies Forced Fast-Leave enabled.

53 indicates port C1.

1 indicates the default VLAN. (See the note on page 4-15.)

Figure 4-6. Example of Changing the Forced Fast-Leave Configuration on Port 53
Using the Switch as Querier

The function of the IGMP Querier is to poll other IGMP-enabled devices in an IGMP-enabled VLAN to elicit group membership information. The switch performs this function if there is no other device in the VLAN, such as a multicast router, to act as Querier. Although the switch automatically ceases Querier operation in an IGMP-enabled VLAN if it detects another Querier on the VLAN, you can also use the switch’s CLI to disable the Querier capability for that VLAN.

**Note**

A Querier is required for proper IGMP operation. For this reason, if you disable the Querier function on a switch, ensure that there is an IGMP Querier (and, preferably, a backup Querier) available on the same VLAN.

If the switch becomes the Querier for a particular VLAN (for example, the DEFAULT_VLAN), then subsequently detects queries transmitted from another device on the same VLAN, the switch ceases to operate as the Querier for that VLAN. If this occurs, the switch Event Log lists a pair of messages similar to these:

```
I 01/15/01 09:01:13 igmp: DEFAULT_VLAN: Other Querier detected
I 01/15/01 09:01:13 igmp: DEFAULT_VLAN: This switch is no longer Querier
```

In the above scenario, if the other device ceases to operate as a Querier on the default VLAN, then the switch detects this change and can become the Querier as long as it is not pre-empted by some other IGMP Querier on the VLAN. In this case, the switch Event Log lists messages similar to the following to indicate that the switch has become the Querier on the VLAN:

```
I 01/15/01 09:21:55 igmp: DEFAULT_VLAN: Querier Election in process
I 01/15/01 09:22:00 igmp: DEFAULT_VLAN: This switch has been elected
```
Excluding Well-Known or Reserved Multicast Addresses from IP Multicast Filtering

Each multicast host group is identified by a single IP address in the range of 224.0.0.0 through 239.255.255.255. Specific groups of consecutive addresses in this range are termed “well-known” addresses and are reserved for pre-defined host groups. IGMP does not filter these addresses, so any packets the switch receives for such addresses are flooded out all ports assigned to the VLAN on which they were received (except the port on which the packets entered the VLAN).

The following table lists the 32 well-known address groups (8192 total addresses) that IGMP does not filter on the Series 5300XL switches, as well as on the 1600M, 2400M, 2424M, 2650M, 4000M, 4100GL, 6108M, 8000M, and Series 2500 switches.

Table 4-2.IP Multicast Address Groups Excluded from IGMP Filtering

<table>
<thead>
<tr>
<th>Groups of Consecutive Addresses in the Range of 224.0.0.X to 239.0.0.X*</th>
<th>Groups of Consecutive Addresses in the Range of 224.128.0.X to 239.128.0.X*</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.x</td>
<td>232.0.0.x</td>
</tr>
<tr>
<td>225.0.0.x</td>
<td>233.0.0.x</td>
</tr>
<tr>
<td>226.0.0.x</td>
<td>234.0.0.x</td>
</tr>
<tr>
<td>227.0.0.x</td>
<td>235.0.0.x</td>
</tr>
<tr>
<td>228.0.0.x</td>
<td>236.0.0.x</td>
</tr>
<tr>
<td>229.0.0.x</td>
<td>237.0.0.x</td>
</tr>
<tr>
<td>230.0.0.x</td>
<td>238.0.0.x</td>
</tr>
<tr>
<td>231.0.0.x</td>
<td>239.0.0.x</td>
</tr>
</tbody>
</table>

* X is any value from 0 to 255.
**Notes:**

**IP Multicast Filters.** *This operation applies to the HP Procurve Series 5300XL switches, as well as on the 1600M, 2400M, 2424M, 4000M, and 8000M, but not to the Series 2500, 2650, Series 4100GL or 6108 switches (which do not have static traffic/security filters).*

IP multicast addresses occur in the range from 224.0.0.0 through 239.255.255.255 (which corresponds to the Ethernet multicast address range of 01005e-000000 through 01005e-7ffffff). Where a switch has a static Traffic/Security filter configured with a “Multicast” filter type and a “Multicast Address” in this range, the switch will use the static filter unless IGMP learns of a multicast group destination in this range. In this case, IGMP dynamically takes over the filtering function for the multicast destination address(es) for as long as the IGMP group is active. If the IGMP group subsequently deactivates, the switch returns filtering control to the static filter.

**Reserved Addresses Excluded from IP Multicast (IGMP) Filtering.**
Traffic to IP multicast groups in the IP address range of 224.0.0.0 to 224.0.0.255 will always be flooded because addresses in this range are “well known” or “reserved” addresses. Thus, if IP Multicast is enabled and there is an IP multicast group within the reserved address range, traffic to that group will be flooded instead of filtered by the switch.

**Number of IP Multicast Addresses Allowed**

Multicast filters and IGMP filters (addresses) together can total up to 255 in the switch. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.
Multimedia Traffic Control with IP Multicast (IGMP)
Excluding Well-Known or Reserved Multicast Addresses from IP Multicast Filtering

This page is intentionally unused.
PIM-DM (Dense Mode)

Contents

Overview ................................................................. 5-2
Introduction ............................................................. 5-3
Feature Overview .......................................................... 5-4
PIM-DM Operation ......................................................... 5-4
  Multicast Flow Management ........................................ 5-7
  General Configuration Elements ................................. 5-9
Terminology ............................................................... 5-9
PIM-DM Operating Rules ............................................... 5-10
Configuring PIM-DM ....................................................... 5-11
  PIM Global Configuration Context ............................ 5-12
  PIM VLAN (Interface) Configuration Context .............. 5-15
Displaying PIM Data and Configuration Settings ............... 5-22
  Displaying PIM Route Data ..................................... 5-23
  Displaying PIM Status ............................................ 5-27
Operating Notes .......................................................... 5-34
Troubleshooting .......................................................... 5-36
Messages Related to PIM Operation ................................. 5-37
Applicable RFCs ............................................................ 5-40
Exceptions to Support for RFC 2932 - Multicast Routing MIB . 5-41
Overview

This chapter describes protocol-independent multicast routing and how to configure it with the switch’s built-in interfaces, and assumes an understanding of multimedia traffic control with IP multicast (IGMP), which is described in the chapter titled “Multimedia Traffic Control with IP Multicast (IGMP)”.

For general information on how to use the switch’s built-in interfaces, refer to these chapters in the Management and Configuration Guide for your switch:

- Chapter 3, “Using the Menu Interface”
- Chapter 4, “Using the Command Line Interface (CLI)”
- Chapter 5, “Using the HP Web Browser Interface”
- Chapter 6, “Switch Memory and Configuration”
## Introduction

- **Configure PIM Global**: n/a, Menu, 5-12, Web
- **Configure PIM VLAN Interface**: n/a, Menu, 5-15, Web
- **Display PIM Route Data**: Disabled, Menu, 5-23, Web
- **Display PIM Status**: 0 (Forward All), Menu, 5-27, Web

In a network where IP multicast traffic is transmitted for multimedia applications, multicast traffic is blocked at routed interface (VLAN) boundaries unless a multicast routing protocol is running. PIM-DM (Protocol Independent Multicasting-Dense Mode, draft version 3) enables and controls multicast traffic routing on the Switch Series 5300XL devices.

PIM-DM is used in networks where, at any given time, multicast group members exist in relatively large numbers and are present in most subnets. PIM-DM operates with any unicast IPv4 routing protocol available on the switch. However, note that PIM-DM uses "flooding" to initially propagate a multicast group to a network, then prunes back the branches that have no hosts requiring membership. For this reason, ample bandwidth is a requirement in PIM-DM applications.

IGMP provides the communication link between a host and the multicast router running PIM. Where hosts are connected directly to the routing device, such as the 5300XL, both PIM and IGMP must run on the switch.
Feature Overview

PIM-DM on the Switch Series 5300XL devices includes:

- **Routing Protocol Support:** PIM uses whichever unicast routing protocol is running on the routing switch. These can include:
  - RIP
  - OSPF
  - Static routes
  - Directly connected interfaces

- **Interface Support:** PIM-DM supports up to 127 outbound VLANs (and 1 inbound VLAN) in its multicast routing table (MRT) at any given time, meaning that the sum of all outbound VLANs across all current flows on a routing switch may not exceed 127. (A single flow may span one inbound VLAN and up to 127 outbound VLANs, depending on the VLAN memberships of the hosts actively belonging to the flow.)

- **IGMP Compatibility:** PIM-DM is compatible with IGMP versions 1 - 3, and is fully interoperable with IGMP for determining multicast flows.

- **XRRP:** PIM-DM is fully interoperable with XRRP to quickly transition multicast routes in the event of a failover.

- **MIB Support:** With some exceptions, PIM-DM supports the parts of the Multicast Routing MIB applicable to PIM-DM operation. (Refer to “Exceptions to Support for RFC 2932 - Multicast Routing MIB” on page 5-41.)

- **PIM Draft Specifications:** Compatible with PIM-DM draft specification, versions 1 and 2.

PIM-DM Operation

PIM-DM operates at the router level to direct traffic for a particular multicast group along the most efficient path to the VLANs having hosts that have joined that group. A unicast source address and a multicast group address comprise a given source/group (S/G) pair. Multicast traffic moving from a source to a multicast group address creates a **flow** to the area(s) of the network requiring the traffic. That is, the flow destination is the multicast group address, and not a specific host or VLAN. Thus, a single multicast flow has one source and one
multicast group address (destination), but may reach many hosts in different
subnets, depending on which hosts have issued joins for the same multicast
group.

PIM routes the multicast traffic for a particular S/G pair on paths between the
source unicast address and the VLANs where it is requested (by joins from
hosts connected to those VLANs). Physical destinations for a particular
multicast group can be hosts in different VLANs or networks. Individual hosts
use IGMP configured per-VLAN to send joins requesting membership in a
particular multicast group. All hosts that have joined a given multicast group
(defined by a multicast address) remain in that group as long as they continue
to issue periodic joins.

On the Switch Series 5300XL devices, PIM-DM interoperates with IGMP and
the switch’s routing protocols. (Note that PIM-DM operates independently of
the routing protocol you choose to run on your switches, meaning you can
use PIM-DM with RIP, OSPF, or static routes configured.) PIM-DM utilizes a
unicast routing table to find the path to the originator of the multicast traffic
and sets up multicast “trees” for distributing multicast traffic. (This method is
termed reverse path forwarding, or RPF).

For the flow of a given multicast group, PIM-DM creates a "tree" structure
between the source and the VLANs where hosts have joined the group. The
tree structure consists of:

- Extended branches to VLANs with hosts that currently belong to the group
- Pruned branches to VLANs with no hosts that belong to the group
When the routing switch detects a new multicast flow, it initially floods the traffic throughout the PIM-DM domain, and then prunes the traffic on the branches (network paths) where joins have not been received from individual hosts. This creates the “tree” structure shown above. The routing switch maintains individual branches in the multicast tree as long as there is at least one host maintaining a membership in the multicast group. When all of the hosts in a particular VLAN drop out of the group, PIM-DM prunes that VLAN from the multicast tree. Similarly, if the routing switch detects a join from a host in a pruned VLAN, it adds that branch back into the tree.

**Note**

Where the multicast routers in a network use one or more multinetted VLANs, there must be at least one subnet common to all routers on the VLAN. This is necessary to provide a continuous forwarding path for the multicast traffic on the VLAN. Refer to the `[all source-ip-address]` option under “PIM VLAN (Interface) Configuration Context” on page 5-15.
Multicast Flow Management

This section provides details on how the routing switch manages forwarding and pruned flows. This information is useful when planning topologies to include multicast support and when viewing and interpreting the “show” command output for PIM-DM features.

Initial Flood and Prune. As mentioned earlier, when a router running PIM-DM receives a new multicast flow, it initially floods the traffic to all downstream multicast routers. PIM-DM then prunes the traffic on paths to VLANs that have no host joins for that multicast address. (Note that PIM-DM does not re-forward traffic back to its source VLAN.)

Maintaining the Prune State. For a multicast group “X” on a given VLAN, when the last host belonging to group “X” leaves the group, PIM places that VLAN in a prune state, meaning the group “X” multicast traffic is blocked to that VLAN. The prune state remains until a host on the same VLAN issues a join for group “X”, in which case the router cancels the prune state and changes the flow to the forwarding state.

State Refresh Packets and Bandwidth Conservation. A 5300XL multicast router, if directly connected to a multicast source such as a video conferencing application, periodically transmits state refresh packets to downstream multicast routers. On routers that have pruned the multicast flow, the state refresh packets keep the pruned state alive. On routers that have been added to the network after the initial flooding and pruning of a multicast group, the state refresh packets inform the newly added router of the current state of that branch. This means that if all multicast routers in a network support the state refresh packet, then the multicast router directly connected to the multicast source performs only one flood-prune cycle to the edge of the network when a new flow (multicast group) is introduced, and preserves bandwidth for other uses. Note, however, that some vendors’ multicast routers do not offer the state refresh feature. In this case, PIM-DM must periodically advertise an active multicast group to these devices by repeating the flood/prune cycle on the paths to such routers. For better traffic management in multicast-intensive networks where some multicast routers do not offer the state refresh feature, you may want to group such routers where the increased bandwidth usage will have the least effect on overall network performance.
These HP 5300XL multicast routers support the state refresh feature but must handle periodic flood-prune cycles for the downstream routers that lack this feature.

These HP 5300XL multicast routers do not have the state refresh feature and thus require periodic flood-prune cycles to advertise active multicast group. In this case it may be better to group these routers on the same multicast tree to avoid the additional flood/prune cycles on the routers that do support state refresh.

Indicates Paths Requiring Periodic Flood-Prune Cycles for a Given Multicast Group

These HP 5300XL multicast routers support the state refresh feature and do not require periodic flood-prune cycles for a given multicast group, which frees up bandwidth for other uses.

Figure 5-2. Example of Bandwidth Conservation in 5300XL Routing Switches with PIM-DM State Refresh
General Configuration Elements

The configured elements PIM-DM requires are:

1. IP routing enabled on all routing switches you want to carry routed multicast traffic.

2. Configure the routing method(s) needed to reach the interfaces (VLANs) on which you want multicast traffic available for hosts in your network:
   - Enable RIP or OSPF at both the global and VLAN levels on the routers where there are connected hosts that may issue multicast joins.
   - Configure static routes to and from the destination subnets.

3. Enable IP multicast routing.

4. For each VLAN on which there are hosts that you want to join multicast groups, enable IGMP on that VLAN. Repeat this action on every switch and router belonging to the VLAN.

5. Enable PIM-DM at the global level on the routing switch and on the VLANs where you want to allow routed multicast traffic.

**Note**

When you initially enable PIM-DM, HP recommends that you leave the PIM-DM configuration parameters at their default settings. You can then assess performance and make configuration changes where a need appears.

Terminology

**Flow:** Multicast traffic moving between a unicast source and a multicast group. One S/G pair is counted as a single flow, regardless of the number of hosts belonging to the related multicast group.

**Host:** A client device that requests multicast traffic by transmitting IGMP “joins” for a specific multicast group, such as a video conferencing application.

**MRT (Multicast Routing Table):** The routing switch creates this table internally to maintain data on each multicast group it supports. The “Show” commands described later in this chapter display MRT data managed in this table.
**PIM-DM (Dense Mode)**

**PIM-DM Operating Rules**

**Multicast Address:** In IP multicast traffic on the switch, this is a single IP address that can be used by a group of related or unrelated clients wanting the same data. A single S/G pair consists of unicast source address and a multicast group address. Sometimes termed a “multicast group address”. See also “Source” and “S/G Pair”.

**Multicast Routing:** A method for transmitting multicast datagrams from a source in one IP network to a multicast address in one or more other IP networks.

**PIM Neighbor:** On a routing switch configured for PIM operation, a PIM neighbor is another PIM-configured routing switch or router that is either directly connected to the first routing switch or connected through networked switches and/or hubs.

**Prune:** To eliminate branches of a multicast tree that have no hosts sending joins to request or maintain membership in that particular multicast group.

**S/G Pair:** The unicast address of the server transmitting the multicast traffic and the multicast address to which the server is transmitting the traffic.

**Source (S):** In IP multicast traffic on the switch, the source (S) is the unicast address of the server transmitting the multicast traffic. A single S/G pair consists of unicast source address and a multicast group address. See also “S/G Pair”.

---

**PIM-DM Operating Rules**

- The routing switch supports 1022 multicast flows in hardware and up to 978 additional flows in software. (For more on this topic, refer to “Flow Capacity” on page 5-35.)

- The multicast routing table (MRT) that PIM-DM creates allows up to 127 outbound VLANs, meaning that at any given time, PIM-DM supports multicast routing across 127 VLANs.

- The routing switch allows one instance of PIM per VLAN. Thus, in networks using multinetted VLANs, all routers on a given VLAN intended to route multicast packets must have a least one common subnet on that VLAN. Thus, in the case of multinetting, you must select one subnet on the multinetted VLAN to use for multicast routing. To facilitate this, the routing switch provides a command for specifying which IP address PIM will use on each VLAN.
# Configuring PIM-DM

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PIM Global Context Commands</strong></td>
<td></td>
</tr>
<tr>
<td>[no] ip multicast routing</td>
<td>5-12</td>
</tr>
<tr>
<td>[no] router pim</td>
<td>5-12</td>
</tr>
<tr>
<td>state-refresh</td>
<td>5-13</td>
</tr>
<tr>
<td>trap</td>
<td>5-13</td>
</tr>
<tr>
<td><strong>PIM Interface Context Commands</strong></td>
<td></td>
</tr>
<tr>
<td>[no] ip pim</td>
<td>5-15</td>
</tr>
<tr>
<td>[&lt; all</td>
<td>source-ip-address &gt;]</td>
</tr>
<tr>
<td>[ hello-interval ]</td>
<td>5-15</td>
</tr>
<tr>
<td>[ hello-delay ]</td>
<td>5-16</td>
</tr>
<tr>
<td>[ graft-retry-interval ]</td>
<td>5-16</td>
</tr>
<tr>
<td>[ max-graft-retries ]</td>
<td>5-17</td>
</tr>
<tr>
<td>[ lan-prune-delay ]</td>
<td>5-17</td>
</tr>
<tr>
<td>[ propagation-delay ]</td>
<td>5-18</td>
</tr>
<tr>
<td>[ override-delay ]</td>
<td>5-18</td>
</tr>
<tr>
<td>[ ttl-threshold ]</td>
<td>5-19</td>
</tr>
</tbody>
</table>
PIM-DM requires configuration on both the global level and on the VLAN (interface) level. The recommended configuration order is:

1. Enable IGMP on all VLANs where hosts may join a multicast group.
2. Enable the following at the global level on the Switch Series 5300XL device.
   - IP routing
   - IP multicast routing
   - Router PIM and any non-default, global PIM settings you want to apply
   - Router RIP, Router OSPF, and/or a static route
3. If you selected RIP or OSPF in step 2, then on each VLAN where you want multicast routing to operate, enable the same option.
4. Enable the following in each VLAN context where you want multicast routing to operate:
   - IP RIP or IP OSPF
   - IP PIM
   - Any non-default, VLAN-level IP PIM settings you want to apply

PIM Global Configuration Context

**Note**

PIM-DM operation requires a routing protocol enabled on the routing switch. You can use RIP, OSPF, and/or static routing. The examples in this section use RIP. For more on these topics, refer to the chapter titled “IP Routing Features” in this guide.

**Syntax:**  
```plaintext
[no] ip multicast-routing
```

*Enables or disables IP multicast routing on the routing switch. IP routing must be enabled. (Default: Disabled.)*

**Syntax:**  
```plaintext
[no] router pim
```

*Enables or disables PIM at the global level. IP routing must be enabled first. (Default: Disabled.)*
**Syntax:** `router pim [state-refresh < 10 - 300 >]`

Sets the interval in seconds between successive State Refresh messages originated by the routing switch. Note that only the routing switch connected directly to the unicast source initiates state-refresh packets. All other PIM routers in the network only propagate these state-refresh packets. (Default: 60 seconds)

**Syntax:** `[no] router pim trap < all | neighbor-loss | hardware-mrt-full | software-mrt-full >`

Enables and disables these PIM SNMP traps:
- `all` — Enable/Disable all PIM notification traps.
- `neighbor-loss` — Enable/Disable the notification trap sent when the timer for a multicast router neighbor expires and the switch has no other multicast router neighbors on the same VLAN with a lower IP address. (Default: Disabled.)
- `hardware-mrt-full` — Enable/Disable notification trap when the hardware multicast routing table (MRT) is full (1023 active flows). In this state, any additional flows are handled by the software MRT, which increases processing time for the affected flows. (Default: Disabled.)
- `software-mrt-full` — Enable/Disable notification trap when the routing switch’s software multicast routing table is full (that is, when routing resources for active flows are exhausted). (Default: Disabled.) Note that in this state, the routing switch does not accept any additional flows.

**Example of Configuring PIM at the Global Level.** In figure 5-1 on page 5-6, the “5308XL #1” routing switch is directly connected to the multicast sources for the network. In this case, suppose that you want to do the following:

- Reduce the state-refresh time from the default 60 seconds to 30 seconds. Note that the routing switch transmits state-refresh packets only if it is directly connected to the multicast source.
- Configure an SNMP trap to notify your network management station if the routing switch’s hardware multicast routing table becomes filled to the maximum of 1023 active flows.
To configure global-level PIM operation for the “5308XL #1” routing switch, you would use the commands shown in figure 5-3, below.

```
HPswitch(config)# ip routing  Enables IP routing.
HPswitch(config)# ip multicast-routing  Enables multicast routing.
HPswitch(config)# router pim  Enables PIM.
HPswitch(pim)# router rip  Enables RIP.
HPswitch(pim)# state-refresh 45  Configures a non-default State Refresh timer.
HPswitch(pim)# trap hardware-mrt-full  Sets an SNMP trap to notify an SNMP management station if the hardware multicast routing table fills with active flows.
HPswitch(pim)# write mem
HPswitch(pim)# exit
```

Using show config displays the configuration changes resulting from the above commands.

```
HPswitch(config)# show config
Startup configuration:
; J4850A Configuration Editor; Created on release #E.08.01
hostname "HPswitch"
module 1 type J4820A
ip routing
snmp-server community "public" Unrestricted
snmp-server host 15.29.38.205 "public" Not-INFO
snmp-server host 15.255.124.84 "public" Not-INFO
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A5,A16,A19
  ip address dhcp-bootp
  no untagged A6-A15,A17-A18,A20-A24
exit
vlan 29
  name "VLAN29"
  :
  :
exit
vlan 25
  name "VLAN25"
  untagged A20-A24
  ip address 25.38.10.1
exit
ip multicast-routing
ip ssh filetransfer
router rip
  exit
  [router pim
  |  trap hardware-mrt-full]
  [  state-refresh 45 ]
  exit
```

Figure 5-3. Example of Configuring PIM-DM on a Routing Switch at the Global Level
After configuring the global-level PIM operation on a routing switch, go to the device’s VLAN context level for each VLAN you want to include in your multicast routing domain. (Refer to “PIM VLAN (Interface) Configuration Context”, below.

### PIM VLAN (Interface) Configuration Context

**Syntax:**

```plaintext
[n] ip pim
[n] vlan < vid > ip pim
```

*Enables multicast routing on the VLAN interface to which the CLI is currently set. The no form disables PIM on the VLAN. Default: Disabled.*

**Syntax:**

```plaintext
[n] ip pim [ all | < source-ip-address > ]
[n] vlan < vid > ip pim [ all | < source-ip-address > ]
```

*In networks using multinetted VLANs, all routers on a given VLAN intended to route multicast packets must have a least one common subnet on that VLAN. Use this command when the VLAN is configured with multiple IP addresses (multinetting) to specify the IP address to use as the source address for PIM protocol packets outbound on the VLAN. Use `< ip-address >` to designate a single subnet in cases where multicast routers on the same multinetted VLAN are not configured with identical sets of subnet IP addresses. Use `< all >` if the multinetted VLAN is configured with the same set of subnet addresses. (Default: The Primary VLAN.)*

**Syntax:**

```plaintext
ip pim [ hello-interval < 5 - 30 > ]
vlan < vid > ip pim [ hello-interval < 5 - 30 >]
```

*Changes the frequency at which the routing switch transmits PIM “Hello” messages on the current VLAN. The routing switch uses “Hello” packets to inform neighboring routers of its presence. The routing switch also uses this setting to compute the **Hello Hold Time**, which is included in Hello packets sent to neighbor routers. **Hello Hold Time** tells neighbor routers how long to wait for the next Hello packet from the routing switch. If another packet does not arrive within that time, the router removes the neighbor adjacency on that VLAN from the routing table, which removes any flows running on that interface. Shortening the Hello interval reduces the Hello Hold Time. This has the effect of changing how quickly other routers will stop sending traffic to the routing switch if they do not receive a new Hello packet when expected.*
For example, if multiple routers are connected to the same VLAN and the routing switch requests multicast traffic, all routers on the VLAN receive that traffic. (Those which have pruned the traffic will drop it when they receive it.) If the upstream router loses contact with the routing switch receiving the multicast traffic (that is, fails to receive a Hello packet when expected), then the shorter Hello Interval causes it to stop transmitting multicast traffic onto the VLAN sooner, resulting in less unnecessary bandwidth usage.

Not used with the no form of the ip pim command.

Syntax:
```
ip pim [ hello-delay < 0 - 5 >]
vl < vid > ip pim [ hello-delay < 0 - 5 >]
```

Changes the maximum time in seconds before the routing switch actually transmits the initial PIM Hello message on the current VLAN. In cases where a new VLAN activates with connections to multiple routers, if all of the connected routers sent Hello packets at the same time, then the receiving router could become momentarily overloaded. This value randomizes the transmission delay to a time between 0 and the hello delay setting. Using “0” means no delay. After the routing switch sends the initial Hello Packet to a newly detected VLAN interface, it sends subsequent Hello packets according to the current Hello Interval setting. Not used with the no form of the ip pim command. Default: 5 seconds.

Syntax:
```
ip pim [ graft-retry-interval < 1-10 >]
vl < vid > ip pim [ graft-retry-interval < 1-10 >]
```

Graft packets result when a downstream router transmits a request to join a flow. The upstream router responds with a graft acknowledgment packet. If the Graft Ack is not received within the time period of the graft-retry-interval, it resends the graft packet. This command changes the interval (in seconds) the routing switch waits for the Graft Ack (acknowledgement) from another router before resending the Graft request. Not used with the no form of the ip pim command. (Default: 3 seconds.)
**Syntax:**
```
ip pim [ max-graft-retries < 1 - 10 >
  vlan < vid > ip pim [ max-graft-retries < 1 - 10 >
```

Changes the number of times the routing switch will retry sending the same graft packet to join a flow. If a Graft Ack response is not received after the specified number of retries, the routing switch ceases trying to join the flow. In this case the flow is removed until either a state refresh from upstream re-initiates the flow or an upstream router floods the flow. Increasing this value helps to improve multicast reliability. Not used with the **no** form of the `ip pim` command. (Default: 3 attempts.)

**Syntax:**
```
ip pim [ lan-prune-delay ]
  vlan < vid > ip pim [ lan-prune-delay ]
```

Enables the LAN Prune Delay option on the current VLAN. With `lan-prune-delay` enabled, the routing switch informs downstream neighbors how long it will wait before pruning a flow after receiving a prune request. Other, downstream routers on the same VLAN must send a Join to override the prune before the `lan-prune-delay` time if they want the flow to continue. This prompts any downstream neighbors with hosts continuing to belong to the flow to reply with a Join. If no joins are received after the `lan-prune-delay` period, the routing switch prunes the flow. The propagation-delay and override-interval settings (below) determine the `lan-prune-delay` setting.

Uses the **no** form of the `ip pim` command to disable the LAN Prune Delay option. (Default: Enabled.)
PIM-DM (Dense Mode)
Configuring PIM-DM

Syntax:

```
ip pim [ propagation-delay < 250-2000 >]
vlan < vid > ip pim [ propagation-delay < 250-2000 >]

ip pim [ override-interval < 500 - 6000 >]
vlan < vid > ip pim [ override-interval < 500 - 6000 >]
```

A routing switch sharing a VLAN with other multicast routers uses these two values to compute the lan-prune-delay setting (above) for how long to wait for a PIM-DM join after receiving a prune packet from downstream for a particular multicast group. For example, a network may have multiple routing switches sharing VLAN “X”. When an upstream routing switch initially floods traffic from multicast group “X” to VLAN “Y”, if one of the routing switches on VLAN “Y” does not want this traffic it issues a prune response to the upstream neighbor. The upstream neighbor then goes into a “prune pending” state for group “X” on VLAN “Y”. (During this period, the upstream neighbor continues to forward the traffic.) During the “pending” period, another routing switch on VLAN “Y” can send a group “X” Join to the upstream neighbor. If this happens, the upstream neighbor drops the “prune pending” state and continues forwarding the traffic. But if no routers on the VLAN send a Join, then the upstream router prunes group “X” from VLAN “Y” when the lan-prune-delay timer expires. (Defaults: propagation-delay = 500 milliseconds; override-interval = 2500 milliseconds.)
**Syntax:**

```
ip pim [ ttl-threshold < 0 - 255 > ]
vlan < vid > ip pim
```

Sets the multicast datagram time-to-live (router hop-count) threshold for the VLAN. Any IP multicast datagrams or state refresh packets with a TTL less than this threshold will not be forwarded out the interface. The default value of 0 means all multicast packets are forwarded out the interface.

This parameter provides a method for containing multicast traffic within a network, or even within specific areas of a network. Initially, the multicast traffic source sets a TTL value in the packets it transmits. Each time one of these packets passes through a multicast routing device, the TTL setting decrements by 1. On a Switch Series 5300XL device, if the packet arrives with a TTL lower than the `mroute ttl-threshold`, the routing switch does not forward the packet.

Changing this parameter on a routing switch requires knowledge of the TTL setting of incoming multicast packets. A value that is too high can allow multicast traffic to go beyond your internal network. A value that is too low may prevent some intended hosts from receiving the desired multicast traffic. (Default: 0 — forwards multicast traffic regardless of packet TTL setting.)

**Example of Configuring PIM-DM Operation at the VLAN Level.** The network in figure 5-4 uses VLAN 25 for multicast traffic. However, this VLAN is multinetted and there is only one subnet (25.38.10.x) in VLAN 25 that is common to all three routing switches. Thus, when configuring VLAN 25 on these routing switches to perform multicast routing, it is necessary to use `ip pim < source-ip-address >` to designate the common subnet as the source address for outbound multicast traffic on VLAN 25. (If only identical subnets were present in the multinetted VLAN 25 configuration on all three devices, then the `ip pim all` command would be used instead.) Note that the other VLANs in the network are not multinetted and therefore do not require the the `ip pim < all | source-ip-address >` option.

For this example, assume that the VLANs and IP addressing are already configured on the routing switch.
On the three routing switches, VLAN 25 is multinetted with subnets that match in only one instance. Since subnet 25.38.10.x exists on VLAN 25 in all routing switches, it serves as the source IP address for multicast traffic outbound on VLAN 25 for the network.

The remaining VLANs (27, 28, 29, and 30) in the network are not multinetted on the routing switches and it is not necessary to configure a source address for multicast routing on these other VLANs.

In this example, the multicast source transmits packets with a TTL (time-to-live) of 192. To prevent these packets from moving beyond routers 2 and 3, you would configure the TTL in the downstream routers (below routers 2 and 3) at 190. (It is not necessary to configure the TTL on routers 1 - 3.)
HPswitch(config)# show config
Startup configuration:

hostname "HPswitch"
module 1 type J4820A

ip routing,

vlan 29
  name "VLAN29"
  untagged A11-A15, A17
  ip address 29.29.30.1 255.255.248.0
  ip igmp,
  exit

vlan 27
  name "VLAN27"
  untagged A6-A10, A18
  ip address 27.27.30.1 255.255.248.0
  ip igmp,
  exit

vlan 25
  name "VLAN25"
  untagged A20-A24
  ip address 25.38.10.1 255.255.255.0
  ip address 25.38.11.1 255.255.255.0
  ip address 25.38.12.1 255.255.255.0
  ip igmp,
  _exit_-------------------------

[ ip multicast-routing ]

[ router rip ]
  _exit ______________________

[ router pim ]
  _exit ______________________

 vlan _25____________________
  ip rip ______________________
  ip pim 25.38.10.1
  _exit ______________________

 vlan _27____________________
  ip rip____________________
  ip pim all
  _exit ______________________

 vlan _29____________________
  ip rip____________________
  ip pim all
  _exit ______________________

Figure 5-6. The Configuration Supporting Multicast Routing on the 5300XL #1 Routing Switch Shown in Figure 5-4 (Page 5-20)
### Displaying PIM Data and Configuration Settings

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip mroute</td>
<td>5-23</td>
</tr>
<tr>
<td>[ interface &lt; vid &gt;]</td>
<td>5-24</td>
</tr>
<tr>
<td>[&lt; multicast-ip-addr&gt; &lt; source-ip-addr &gt;]</td>
<td>5-25</td>
</tr>
<tr>
<td>show ip pim</td>
<td>5-27</td>
</tr>
<tr>
<td>[ interface [&lt; vid ] ]</td>
<td>5-28</td>
</tr>
<tr>
<td>[ mroute [&lt; multicast-group-address&gt; &lt; multicast-source-address &gt;] ]</td>
<td>5-30</td>
</tr>
<tr>
<td>neighbor</td>
<td>5-33</td>
</tr>
<tr>
<td>[&lt; ip-address &gt;]</td>
<td>5-34</td>
</tr>
</tbody>
</table>
Displaying PIM Route Data

**Syntax:** show ip mroute

*Without parameters, lists all VLANs actively forwarding routed, multicast traffic.*

**Group Address:** The multicast address of the specific multicast group (flow).

**Source Address:** The unicast address of the multicast group source.

**Neighbor:** The IP address of the upstream multicast router interface (VLAN) from which the multicast traffic is coming. A blank field for a given multicast group indicates that the multicast server is directly connected to the routing switch.

**VLAN:** The interface on which the multicast traffic is moving.

For example, the next figure displays the show ip route output on the “5300XL #2” routing switch in figure 5-4 on page 5-20. This case illustrates two multicast groups from the same multicast server source.

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Neighbor</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>239.255.255.1</td>
<td>27.27.30.2</td>
<td>29.29.30.1</td>
<td>29</td>
</tr>
<tr>
<td>239.255.255.5</td>
<td>27.27.30.2</td>
<td>29.29.30.1</td>
<td>29</td>
</tr>
</tbody>
</table>

Figure 5-7. Example Showing the Route Entry Data on the “5300XL #2” Routing Switch in Figure 5-4 on Page 5-20
Syntax:  show ip mroute [ interface < vid >]

Lists these settings:

**VLAN:** The VID specified in the command.

**Protocol Identity:** PIM-DM only.

**TTL:** The time-to-live threshold for packets forwarded through this VLAN. When configured, the routing switch drops multicast packets having a TTL lower than this value. (When a packet arrives, the routing switch decrements it’s TTL by 1, then compares the decremented packet TTL to the value set by this command.) A **TTL Threshold** setting of 0 (the default) means all multicast packets are forwarded regardless of the TTL value they carry. A multicast packet must have a TTL greater than 1 when it arrives at the routing switch. Otherwise the routing switch drops the packet instead of forwarding it on the VLAN.

```
HPswitch(config)# show ip mroute interface 29

IP Multicast Interface

VLAN : 29
Protocol : PIM-DM

TTL Threshold : 0
```

Figure 5-8. Example of the Above Command on the “5300XL #2” Routing Switch in Figure 5-4 on Page 5-20
Syntax: show ip mroute [<multicast-ip-addr> <source-ip-addr>]

Lists the following data for the specified flow (multicast group):

**Group Address:** The multicast group IP address for the current group.

**Source Address:** The multicast source address `<source-ip-addr>` for the current group.

**Source Mask:** The subnet mask applied to the multicast source address `<source-ip-addr>`.

**Neighbor:** Lists the IP address of the upstream next-hop router running PIM-DM; that is, the router from which the routing switch is receiving datagrams for the current multicast group. This value is **0.0.0.0** if the routing switch has not detected the upstream next-hop router’s IP address. This field is empty if the multicast server is directly connected to the routing switch.

**VLAN:** Lists the VLAN ID (VID) on which the routing switch received the specified multicast flow.

**Up Time (Sec):** The elapsed time in seconds since the routing switch learned the information for the current instance of the indicated multicast flow.

**Expiry Time (Sec):** Indicates the remaining time in seconds before the routing switch ages-out the current flow (group membership). This value decrements until:

- **Reset by a state refresh packet originating from the upstream multicast router.** (The upstream multicast router issues state refresh packets for the current group as long as it continues to receive traffic for the current flow or receives state refresh packets for the current flow from another upstream multicast router.)
- **Reset by a new flow for the current multicast group on the VLAN.**
- **The timer expires (reaches 0).** In this case the switch has not received either a state refresh packet or new traffic for the current multicast group, and ages-out (drops) the group entry.
**Multicast Routing Protocol:** Identifies the multicast routing protocol through which the current flow was learned.

**Unicast Routing Protocol:** Identifies the routing protocol through which the routing switch learned the upstream interface for the current multicast flow. The listed protocol will be either RIP, OSPF, or Static Route.

**Downstream Interfaces:**

**VLAN:** Lists the VID of the VLAN that the routing switch is using to send the outbound packets of the current multicast flow to the next-hop router.

**State:** Indicates whether the outbound VLAN and next-hop router for the current multicast flow are receiving datagrams.

- **Pruned:** The routing switch has not detected any joins from the current multicast flow and is not currently forwarding datagrams in the current VLAN.
- **Forwarding:** The routing switch has received a join for the current multicast flow and is forwarding datagrams in the current VLAN.

**Up Time (Sec):** Indicates the elapsed time in seconds since the routing switch learned the displayed information about the current multicast flow.

**Expiry Time:** Shows the remaining time in seconds until the Next-Hop routing switch ages-out the current flow (group membership) on the indicated VLAN. Includes the date calculated for the age-out event. This value decrements until:

- **Reset by a state refresh packet originating from the upstream multicast router.** (The upstream multicast router issues state refresh packets for the current group as long as it either continues to receive traffic for the current flow or receives state refresh packets for the current flow from another upstream multicast router.
- **Reset by a new flow for the current multicast group on the VLAN.**
- **The timer expires (reaches 0).** In this case the switch has not received either a state refresh packet or new traffic for the current multicast group, and ages-out (drops) the group entry.

Note that the “Next-Hop routing switch” is the next multicast routing switch in the path from the current multicast routing switch to the source for the displayed multicast flow.
PIM-DM (Dense Mode)
Displaying PIM Data and Configuration Settings

PIM-DM (Dense Mode)
Displaying PIM Data and Configuration Settings

A blank Neighbor field indicates that the multicast server is directly connected to the routing switch.

Figure 5-9. Example Output for “5300XL #1” Routing Switch in Figure 5-4 on Page 5-20

Displaying PIM Status

Syntax: show ip pim

Displays PIM status and global parameters.
PIM Status: Shows either enabled or disabled.
State Refresh Interval (sec): A PIM routing switch originates state refresh messages to inform its neighbors of the active flows it is currently routing. This updates the current flow data on PIM routers that join or rejoin a multicast network after the initial flood and prune. This enables hosts on such routers to join a multicast group without having to wait for a “flood and prune” cycle. PIM routers having the state refresh capability can eliminate all but an initial flood and prune cycle. PIM routers without this capability periodically trigger a flood and prune cycle on the path between the PIM router and the multicast source. (Range: 10 - 300 seconds; Default: 60 seconds.)
Traps: Enables the following SNMP traps:
  - neighbor-loss: Sends a trap if a neighbor router is lost.
  - hardware-mrt-full: Sends a trap if the hardware multicast router (MRT) table is full (511 active flows).
  - software-mrt-full: Sends a trap if the software multicast router (MRT) table is full (511 active flows). This can occur only if the hardware MRT is also full.
  - all: Enables all of the above traps.
Syntax: show ip pim [interface]

Lists the PIM interfaces (VLANs) currently configured in the routing switch.

**VLAN:** Lists the VID of each VLAN configured on the switch to support PIM-DM.

**IP Address:** Lists the IP addresses of the PIM interfaces (VLANs).

**Mode:** Shows dense only.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>IP Address</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>25.38.10.1</td>
<td>dense</td>
</tr>
<tr>
<td>27</td>
<td>27.27.30.1</td>
<td>dense</td>
</tr>
<tr>
<td>29</td>
<td>29.29.30.1</td>
<td>dense</td>
</tr>
</tbody>
</table>

Figure 5-10. Example Output for the “5304XL #1” Routing Switch in Figure 5-4 on Page 5-20

Figure 5-11. Example Output for the “5304XL #1” Routing Switch in Figure 5-4 on Page 5-20
Syntax:  show ip pim [interface [< vid >]]

Displays the current configuration for the specified VLAN (PIM interface). Refer to table 5-1, below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default</th>
<th>Control Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>n/a</td>
<td>vlan &lt; vid &gt; ip pim</td>
</tr>
<tr>
<td>IP</td>
<td>n/a</td>
<td>vlan &lt; vid &gt; ip pim &lt; all</td>
</tr>
<tr>
<td>Mode</td>
<td>dense</td>
<td>n/a; PIM Dense only</td>
</tr>
<tr>
<td>Hello Interval (sec)</td>
<td>30</td>
<td>ip pim hello interval &lt; 5 - 30 &gt;</td>
</tr>
<tr>
<td>Hello Hold Time</td>
<td>105</td>
<td>The routing switch computes this value from the current “Hello Interval” and includes it in the “Hello” packets the routing switch sends to neighbor routers. Neighbor routers use this value to determine how long to wait for another Hello packet from the routing switch. Refer to the description of the Hello Interval on page 5-15.</td>
</tr>
<tr>
<td>Hello Delay</td>
<td>5</td>
<td>vlan &lt; vid &gt; ip pim hello delay &lt; 0 - 5 &gt;</td>
</tr>
<tr>
<td>Graft Retry Interval (sec)</td>
<td>3</td>
<td>vlan &lt; vid &gt; ip pim graft-retry-interval &lt; 1 - 10 &gt;</td>
</tr>
</tbody>
</table>
PIM-DM (Dense Mode)
Displaying PIM Data and Configuration Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Default</th>
<th>Control Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Graft Retries</td>
<td>2</td>
<td>vlan &lt; vid &gt; ip pim graft-retries &lt; 1 - 10 &gt;</td>
</tr>
<tr>
<td>Override Interval</td>
<td>2500</td>
<td>vlan &lt; vid &gt; ip pim override-interval &lt; 500 - 6000 &gt;</td>
</tr>
<tr>
<td>(msec)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Propagation Delay</td>
<td>500</td>
<td>vlan &lt; vid &gt; ip pim propagation-delay &lt; 250-2000 &gt;</td>
</tr>
<tr>
<td>(msec)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SR TTL Threshold</td>
<td>0</td>
<td>vlan &lt; vid &gt; ip pim ttl-threshold &lt; 0 - 255 &gt;</td>
</tr>
<tr>
<td>(router hops)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN Prune Delay</td>
<td>Yes</td>
<td>vlan &lt; vid &gt; ip pim lan-prune-delay</td>
</tr>
<tr>
<td>LAN Delay Enabled</td>
<td>No</td>
<td>Shows Yes if all multicast routers on the current VLAN interface enabled LAN-prune-delay. Otherwise shows No.</td>
</tr>
<tr>
<td>State Refresh</td>
<td>n/a</td>
<td>Indicates whether the VLAN responds to state refresh packets. The VLAN connected to the multicast source does not receive state refresh packets and thus is not state-refresh capable. Downstream VLANs in Switch Series 5300XL devices are state-refresh capable.</td>
</tr>
<tr>
<td>Capable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Syntax: show ip pim [mroute]

Shows PIM-specific information from the IP multicast routing table (IP MRT). When invoked without parameters, lists all PIM entries currently in the routing switch’s IP MRT.

**Group Address:** Lists the multicast group addresses currently active on the routing switch.

**Source Address:** Lists the multicast source address for each Group Address.

**Metric:** Indicates the path cost upstream to the multicast source. Used when multiple multicast routers contend to determine the best path to the multicast source. The lower the value, the better the path. This value is set to 0 (zero) for directly connected routes.

**Metric Pref:** Used when multiple multicast routers contend to determine the path to the multicast source. When this value differs between routers, PIM selects the router with the lowest value. If Metric Pref is the same between contending multicast routers, then PIM selects the router with the lowest Metric value to provide the path for the specified multicast traffic. This value is set to 0 (zero) for directly connected routes.

(Metric Pref is based on the routing protocol in use: RIP, OSPF, or static routing. Also, different vendors may assign different values for this setting.)
PIM-DM (Dense Mode)
Displaying PIM Data and Configuration Settings

This output shows the routing switch is receiving two multicast groups from an upstream device at 27.27.30.2. The "0" metric shows that the routing switch is directly connected to the multicast source.

```
HPswitch# show ip pim mroute
PIM Route Entries

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>Metric</th>
<th>Metric Pref</th>
</tr>
</thead>
<tbody>
<tr>
<td>239.255.255.1</td>
<td>27.27.30.2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>239.255.255.5</td>
<td>27.27.30.2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Figure 5-13. Example Showing a Routing Switch Detecting two Multicast Groups from a Directly Connected Multicast Server

Syntax: show ip pim [mroute [<multicast-group-address> <multicast-source-address>]]

Displays the PIM route entry information for the specified multicast group (flow):

- **Group Address**: Lists the specified multicast group address.
- **Source Address**: Lists the specified multicast source address.
- **Source Mask**: Lists the network mask for the multicast source address.
- **Metric**: Lists the number of multicast router hops to the source address.
- **Metric**: Indicates the path cost upstream to the multicast source. Used when multiple multicast routers contend to determine the best path to the multicast source. The lower the value, the better the path.
- **Metric Pref**: Used when multiple multicast routers contend to determine the path to the multicast source. When this value differs between routers, PIM selects the router with the lowest value. If Metric Pref is the same between contending multicast routers, then PIM selects the router with the lowest Metric value to provide the path for the specified multicast traffic. (Different vendors assign differing values for this setting.)
- **Assert Timer**: The time remaining until the routing switch ceases to wait for a response from another multicast router to negotiate the best path back to the multicast source. If this timer expires without a response from any contending multicast routers, then the routing switch assumes it is the best path, and the specified multicast group traffic will flow through the routing switch.
DownStream Interfaces:
- **VLAN**: Lists the VID of the destination VLAN on the next-hop multicast router.
- **Prune Reason**: Identifies the reason for pruning the flow to the indicated VLAN:
  - **Prune**: A neighbor multicast router has sent a prune request.
  - **Assert**: Another multicast router connected to the same VLAN has been elected to provide the path for the specified multicast group traffic.
  - **Other**: Used where the VLAN is in the pruned state for any reason other than the above two reasons (such as no neighbors exist and no directly connected hosts have done joins).

```
HPswitch# show ip pim mroute 239.255.255.1 27.27.30.2
PIM Route Entry
  Group Address : 239.255.255.1
  Source Address : 27.27.30.2
  Source Mask : 255.255.248.0
  Metric : 3
  Metric Pref : 120
  Assert Timer : 0

DownStream Interfaces
  VLAN Prune Reason
      --------
     28     prune
```

Figure 5-14. Example From the “5304XL #1” Routing Switch in Figure 5-4 on Page 5-20 Showing a Multicast Group from a Directly Connected Source
Syntax:  show ip pim [neighbor]

Lists PIM neighbor information for all PIM neighbors connected to the routing switch:

**IP Address:** Lists the IP address of a neighbor multicast router.

**VLAN:** Lists the VLAN through which the routing switch connects to the indicated neighbor.

**Up Time:** Shows the elapsed time during which the neighbor has maintained a PIM route to the routing switch.

**Expiry Time:** Indicates how long before the routing switch ages-out the current flow (group membership). This value decrements until:

- Reset by a state refresh packet originating from the upstream multicast router. (The upstream multicast router issues state refresh packets for the current group as long as it either continues to receive traffic for the current flow or receives state refresh packets for the current flow from another upstream multicast router.
- Reset by a new flow for the current multicast group on the VLAN.

The timer expires (reaches 0). In this case the switch has not received either a state refresh packet or new traffic for the current multicast group, and ages-out (drops) the group entry.

If the IP-ADDR is specified then detailed information for the specified neighbor is shown.

This example simulates output from the “5304XL #1” Routing Switch in Figure 5-4 on Page 5-20. The data identifies the first downstream neighbor (“5300XL #2”).

```
HPswitch# show ip pim neighbor

PIM Neighbors

<table>
<thead>
<tr>
<th>IP Address</th>
<th>VLAN</th>
<th>Up Time (sec)</th>
<th>Expiry Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>29.29.30.2</td>
<td>29</td>
<td>196</td>
<td>89</td>
</tr>
</tbody>
</table>
```

Figure 5-15. Example of PIM Neighbor Output
**Syntax:**  show ip pim [neighbor [< ip-address >]]

*Lists the same information as show ip pim neighbor (page 5-33) for the specified PIM neighbor:*

<table>
<thead>
<tr>
<th>HPswitch # show ip pim neighbor 29.29.30.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM Neighbor</td>
</tr>
<tr>
<td>IP Address : 29.29.30.2</td>
</tr>
<tr>
<td>VLAN : 29</td>
</tr>
<tr>
<td>Up Time (sec) : 26</td>
</tr>
<tr>
<td>Expiry Time (sec) : 79</td>
</tr>
</tbody>
</table>

*Figure 5-16. Example from the “5304XL #1” Routing Switch in Figure 5-4 on Page 5-20 Showing a Specific Neighbor (“5300XL #2”)*

---

**Operating Notes**

**PIM Routers without State Refresh Messaging Capability.** A PIM router without a state refresh messaging capability learns of currently active flows in a multicast network through periodic flood and prune cycles on the path back to the source. The Switch Series 5300XL devices sense downstream multicast routers that do not have the state refresh capability and will periodically flood active multicast groups to these devices. This periodic flooding is not necessary if all of the downstream multicast routers are HP ProCurve 5300XL devices. (The HP ProCurve Routing Switch Series 9300 and the routers offered by some other vendors do not offer the state refresh capability.)
**Flow Capacity.** The routing switch provides an ample multicast environment, supporting 1022 multicast flows in hardware across a maximum of 64 VLANs. (A flow comprises a unicast source address and a multicast group address, regardless of the number of active hosts belonging to the multicast group at any given time.) While the typical multicast environment should not normally exceed 1022 flows, the routing switch can support up to 978 additional flows in software, depending on available system resources. (Because the switch processes flows in hardware much faster than in software, you may notice slower processing times for flows occurring in software.) Also, while the routing switch can support up to 2,000 flows, the total demand on system resources from the combined use of more than 1,022 simultaneous flows, a high number of VLANs supporting multicast routing, and/or other, resource-intensive features can oversubscribe memory resources, which reduces the number of flows the routing switch can support in software. That is, the switch does not route flows in software that oversubscribe current memory resources. If the routing switch regularly exceeds the hardware limit of 1022 flows and begins routing flows in software, you may want to move some hosts that create multicast demand to another routing switch, or reduce the number of VLANs on the routing switch by moving some VLANs to another routing switch. Note that the routing switch generates a log message if it either routes a flow in software or drops a flow intended for software routing because memory is oversubscribed. (Refer to “Messages Related to PIM Operation” on page 5-37.)

**IGMP Traffic High-Priority Disabled.** Enabling IP multicast routing to support PIM-DM operation has the effect of disabling IGMP traffic high-priority, if configured. (Refer to “Configuring IGMP Traffic Priority” on page 4-10.)

**ACLs and PIM.** The switch allows ACL filtering on unicast addresses, but not on multicast addresses. Also, an ACL does not take effect on a flow if the flow began before the ACL was configured.

**When To Enable IGMP on a VLAN.** When PIM is enabled on a VLAN, it is not necessary to also enable IGMP unless there may be Joins occurring on that VLAN. But if IGMP is enabled on a VLAN, you must also enable PIM if you want that VLAN to participate in multicast routing.

**IP Address Removed.** If you remove the IP address for a VLAN, the switch automatically removes the PIM configuration for that VLAN.
Troubleshooting

Symptom: Noticeable slowdown in some multicast traffic. If the switch is supporting more than 1022 active flows. This generates the message Unable to learn HW IP multicast groups, table FULL in the Event Log because there is no room in the hardware Multicast Routing Table to add another Multicast Group. Software will route any multicast packets sent to multicast groups that are not in the hardware Multicast Routing Table, but it will be slower and packets may be dropped if the data rate is greater than 3000 packets per second. Refer to “Flow Capacity” on page 5-35.

Note that the PIM protocol uses one MRT entry for every IP multicast source/group pair that it is routing. An entry is not used if the multicast flow is bridged and not routed. Entries in this table are automatically aged out if they are unused for a period of time.

IPv4 Table Operation. The IPv4 table, which contains the active IP multicast addresses the switch is currently supporting, has 128k entries. However, the IPv4 table also contains IP host entries for every IP source or destination that the switch has learned, as well as ACL flow entries. Entries in this table are generally aged out if they are unused for 5 minutes or more.
Messages Related to PIM Operation

These messages appear in the Event Log and, if Syslog Debug is configured, in the designated Debug destinations.

**Note**
The `<counter>` value displayed at the end of each PIM Event Log message (and SNMP trap messages, if trap receivers are configured) indicates the number of times the switch has detected a recurring event since the last reboot. For more information, refer to “Using the Event Log To Identify Problem Sources” in the “Troubleshooting” appendix of the February, 2004 (or later) version of the Management and Configuration Guide for your switch.

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;alpha-string&gt;</code> pkt, src IP <code>&lt;ip-addr&gt;</code> vid <code>&lt;vlan-id&gt;</code> (not a nbr) <code>&lt;counter&gt;</code></td>
<td>A PIM packet arrived from another router for which no neighbor was found. May indicate a misconfiguration between the sending and receiving router. May also occur if a connected router is disconnected, then reconnected.</td>
</tr>
<tr>
<td>Bad TTL in State Refresh pkt from IP <code>&lt;source-ip-addr&gt;</code> <code>&lt;counter&gt;</code></td>
<td>The switch detected a TTL of 0 (zero) in the PIM portion of a state refresh packet. (Note that this is not the IP TTL.)</td>
</tr>
<tr>
<td>Failed alloc of HW <code>&lt;alpha-str&gt;</code> for flow <code>&lt;multicast-address&gt;</code>, <code>&lt;source-address&gt;</code> <code>&lt;dup-msg-cnt&gt;</code></td>
<td>There are more than 1022 active flows. The switch routes the excess through software, which processes traffic at a slower rate. If this will be an ongoing or chronic condition, transfer some of the flows to another router.</td>
</tr>
<tr>
<td>Failed to alloc a PIM <code>&lt;data-type&gt;</code> pkt <code>&lt;counter&gt;</code></td>
<td>The router was unable to allocate memory for a PIM control packet. Router memory is oversubscribed. Reduce the number of VLANs or increase the hello delay and/or the override interval to reduce the number of simultaneous packet transmissions. Note that if the number of flows exceeds 1022, the excess flows are routed in software, which reduces the number of packet transmissions. In this case, reducing the number of flows by moving some clients to other routers can help.</td>
</tr>
<tr>
<td>Failed to initialize <code>&lt;text-str&gt;</code> as a call back routine <code>&lt;counter&gt;</code></td>
<td>Indicates an internal error. Report the incident to your HP customer care center and re-install the router software.</td>
</tr>
<tr>
<td>I/F configured with IP <code>&lt;ip-address&gt;</code> on vid <code>&lt;vlan-id&gt;</code> <code>&lt;counter&gt;</code></td>
<td>Indicates that the interface (VLAN) has been configured with the indicated primary IP address. At boot-up or when a primary IP address is changed, the switch generates this message for each PIM-configured VLAN.</td>
</tr>
<tr>
<td>Message</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>I/F removal with IP <code>&lt;ip-addr&gt;</code> on vid <code>&lt;vlan-id&gt;</code> <code>&lt;counter&gt;</code></td>
<td>Indicates that a PIM interface (VLAN) has been removed from the router as a result of a primary IP address change or removal.</td>
</tr>
</tbody>
</table>
| MCAST flow `<multicast-address>` `<source-address>` not rteing (rsc low) `<counter>` | The indicated multicast flow is not routing. The routing switch is low on memory resources as a result of too many flows for the number of configured VLANs. Remedies include one or more of the following:  
  • Reduce the number of configured VLANs by moving some VLANs to another router.  
  • Free up system resources by disabling another feature, such as one of the spanning-tree protocols or either the RIP or the OSPF routing protocol. (Unless you are using static routes, you will need to retain a minimum of one unicast routing protocol.) Another option that may help is to reduce the number of configured QoS filters.  
  • Move some hosts that create multicast demand to another router. |
| MCAST MAC add for `<mac-address>` failed `<counter>` | Indicates a hardware problem. Check the cabling and router ports. |
| Multicast Hardware Failed to Initialize `<counter>` | Indicates a hardware failure that halts hardware processing of PIM traffic. The software will continue to process PIM traffic at a slower rate. Contact your HP customer care center. |
| No IP address configured on VID `<vlan-id>` `<dup-msg-cnt>` | PIM has detected a VLAN without an IP address. Configure an IP address on the indicated VLAN. |
| Pkt dropped from `<ip-address>`, `<cause>` vid `<vlan-id>` `<counter>` | A PIM packet from `<ip-address>` was dropped due to one of the following causes:  
  • No PIM interface on the VLAN  
  • Bad packet length  
  • Bad IP header length  
  • Bad IP total length |
<p>| Pkt rcvd with a cksum error from <code>&lt;ip-addr&gt;</code> <code>&lt;counter&gt;</code> | A packet having a checksum error was received from <code>&lt;ip-addr&gt;</code>. Check the cabling and ports on the local and the remote routers. |
| Rcvd incorrect hello from <code>&lt;ip-addr&gt;</code> <code>&lt;counter&gt;</code> | Indicates receipt of a malformed hello packet. (That is, the packet does not match the current specification.) Ensure that compatible versions of PIM-DM are being used. |
| Rcvd <code>&lt;text-str&gt;</code> pkt with bad len from <code>&lt;ip-addr&gt;</code> <code>&lt;counter&gt;</code> | A peer router may be sending incorrectly formatted PIM packets. |
| Rcvd hello from <code>&lt;ip-address&gt;</code> on vid <code>&lt;vlan-id&gt;</code> <code>&lt;counter&gt;</code> | Indicates a misconfiguration where two routers are directly connected with different subnets on the same connected interface. |</p>
<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rcvd pkt from rtr &lt; ip-address &gt;, unkwn pkt type &lt; value &gt; (&lt;counter&gt;)</td>
<td>A packet received from the router at &lt; ip-address &gt; is an unknown PIM packet type. (The &lt; value &gt; variable is the numeric value received in the packet.)</td>
</tr>
<tr>
<td>Rcvd pkt ver# &lt; ver-num &gt;, from &lt; ip-address &gt;, expected &lt; ver-num &gt; (&lt;counter&gt;)</td>
<td>The versions of PIM-DM on the sending and receiving routers do not match. Differing versions will typically be compatible, but features not supported in both versions will not be available.</td>
</tr>
<tr>
<td>Rcvd unkwn addr fmly &lt; addr-type &gt; in &lt; text-str &gt; pkt from &lt; ip-addr &gt; (&lt;counter&gt;)</td>
<td>The router received a PIM packet with an unrecognized encoding. As of February, 2004, the router recognizes IPv4 encoding.</td>
</tr>
<tr>
<td>Rcvd unkwn opt &lt; opt-nbr &gt; in &lt; text-string &gt; pkt from &lt; ip-addr &gt; (&lt;counter&gt;)</td>
<td>The router received a PIM packet carrying an unknown PIM option. The packet may have been generated by a newer version of PIM-DM, or is corrupt. In most cases, normal PIM-DM operation will continue.</td>
</tr>
<tr>
<td>Send error(&lt; failure-type &gt;) on &lt; packet-type &gt; pkt on VID &lt; vid &gt; (&lt;counter&gt;)</td>
<td>Indicates a send error on a packet. This can occur if a VLAN went down right after the packet was sent. The message indicates the failure type, the packet type, and the VLAN ID on which the packet was sent.</td>
</tr>
<tr>
<td>Unable to alloc &lt; text-str &gt; table (&lt;counter&gt;)</td>
<td>The router was not able to create some tables PIM-DM uses. Indicates that the router is low on memory resources. Remedies include one or more of the following:</td>
</tr>
<tr>
<td>• Reduce the number of configured VLANs by moving some VLANs to another router.</td>
<td></td>
</tr>
<tr>
<td>• Free up system resources by disabling another feature, such as one of the spanning-tree protocols or either the RIP or the OSPF routing protocol. (Unless you are using static routes, you will need to retain a minimum of one unicast routing protocol.) Another option that may help is to reduce the number of configured QoS filters.</td>
<td></td>
</tr>
<tr>
<td>• Move some hosts that create multicast demand to another router.</td>
<td></td>
</tr>
<tr>
<td>Unable to alloc a buf of size &lt; bytes &gt; for &lt; data-flow &gt; (&lt;counter&gt;)</td>
<td>Multicast routing is unable to acquire memory for a flow. Router memory is oversubscribed. Reduce the number of VLANs or the number of features in use. Remedies include one or more of the following:</td>
</tr>
<tr>
<td>• Reduce the number of configured VLANs by moving some VLANs to another router.</td>
<td></td>
</tr>
<tr>
<td>• Free up system resources by disabling another feature, such as one of the spanning-tree protocols or either the RIP or the OSPF routing protocol. (Unless you are using static routes, you will need to retain a minimum of one unicast routing protocol.) Another option that may help is to reduce the number of configured QoS filters.</td>
<td></td>
</tr>
<tr>
<td>• Move some hosts that create multicast demand to another router.</td>
<td></td>
</tr>
</tbody>
</table>
## PIM-DM (Dense Mode)

### Applicable RFCs

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| Unable to alloc a msg buffer for `<text-message>` ( `<counter>` ) | Multicast routing is unable to acquire memory for a flow. Router memory is oversubscribed. Reduce the number of VLANs or the number of features in use. Remedies include one or more of the following:  
  - Reduce the number of configured VLANs by moving some VLANs to another router.  
  - Free up system resources by disabling another feature, such as one of the spanning-tree protocols or either the RIP or the OSPF routing protocol. (Unless you are using static routes, you will need to retain a minimum of one unicast routing protocol.) Another option that may help is to reduce the number of configured QoS filters.  
  - Move some hosts that create multicast demand to another router. |

### Applicable RFCs

PIM on the Switch Series 5300XL devices is compatible with these RFCs:

- RFC 3376 - Internet Group Management Protocol, Version 3
- RFC 2365 - Administratively Scoped IP Multicast
- RFC 2932 - Multicast Routing MIB, with exceptions (Refer to "Exceptions to Support for RFC 2932 - Multicast Routing MIB").
- RFC 2933 - IGMP MIB
- RFC 2934 - Protocol Independent Multicast MIB for IPv4
- draft-ietf-ssm-arch-01.txt - Source-Specific Multicast for IP (draft specification, expires May 2003)
Exceptions to Support for RFC 2932 - Multicast Routing MIB

These MIB objects are not supported in the 5300XL routing switch.

- ipMRouteInterfaceRateLimit
- ipMRouteInterfaceInMcastOctets
- ipMRouteInterfaceOutMcastOctets
- ipMRouteInterfaceHCMcastOctets
- ipMRouteInterfaceHCOutMcastOctets
- ipMRouteBoundaryTable
- ipMRouteBoundaryEntry
- ipMRouteBoundaryIfIndex
- ipMRouteBoundaryAddress
- ipMRouteBoundaryAddressMask
- ipMRouteBoundaryStatus
- ipMRouteScopeNameTable
- ipMRouteScopeNameEntry
- ipMRouteScopeNameAddress
- ipMRouteScopeNameAddressMask
- ipMRouteScopeNameLanguage
- ipMRouteScopeNameString
- ipMRouteScopeNameDefault
- ipMRouteScopeNameStatus
Spanning-Tree Operation

Contents

Overview ................................................................. 6-2
The RSTP (802.1w) and STP (802.1D) Spanning Tree Options ... 6-5
Configuring Rapid Reconfiguration Spanning Tree (RSTP) .... 6-9
802.1D Spanning-Tree Protocol (STP) ............................. 6-21
  Menu: Configuring 802.1D STP .................................. 6-21
  CLI: Configuring 802.1D STP .................................. 6-24
  STP Fast Mode .................................................... 6-28
  Fast-Uplink Spanning Tree Protocol (STP) ...................... 6-29
Web: Enabling or Disabling STP .................................... 6-43
802.1s Multiple Spanning Tree Protocol (MSTP) .................. 6-44
  MSTP Structure .................................................... 6-45
  How MSTP Operates ............................................. 6-47
  Terminology ....................................................... 6-50
  Operating Rules ................................................. 6-52
  Transitioning from STP or RSTP to MSTP ...................... 6-53
  Tips for Planning an MSTP Application ......................... 6-54
  Steps for Configuring MSTP .................................... 6-55
  Configuring MSTP Operation Mode and Global Parameters .... 6-57
  Configuring Basic Port Connectivity Parameters ............... 6-61
  Configuring MST Instance Parameters ........................ 6-63
  Configuring MST Instance Per-Port Parameters ................ 6-66
  Enabling or Disabling Spanning Tree Operation ................. 6-69
  Enabling an Entire MST Region at Once or Exchanging One
  Region Configuration for Another ............................. 6-69
  Displaying MSTP Statistics and Configuration ................ 6-71
  Operating Notes .................................................. 6-78
  Troubleshooting .................................................. 6-78
# Overview

## STP Features

<table>
<thead>
<tr>
<th>802.1D Spanning Tree Protocol</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing the STP Configuration</td>
<td>n/a</td>
<td>page 6-21</td>
<td>page 6-12</td>
<td>—</td>
</tr>
<tr>
<td>Enable/Disable STP</td>
<td>Disabled</td>
<td>page 6-21</td>
<td>page 6-25</td>
<td>page 6-43</td>
</tr>
<tr>
<td>Reconfiguring General Operation</td>
<td>priority: 32768 max age: 20 s hello time: 2 s fwd. delay: 15 s</td>
<td>page 6-21</td>
<td>page 6-26</td>
<td>—</td>
</tr>
<tr>
<td>Reconfiguring Per-Port STP</td>
<td>path cost: var priority: 128 mode: norm</td>
<td>page 6-21</td>
<td>page 6-27</td>
<td>—</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>802.1w Spanning Tree Protocol</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing the RSTP/STP Configuration</td>
<td>n/a</td>
<td>page 6-18</td>
<td>page 6-12</td>
<td>—</td>
</tr>
<tr>
<td>Enable/Disable RSTP/STP (RSTP is selected as the default protocol.)</td>
<td>Disabled</td>
<td>page 6-18</td>
<td>page 6-13</td>
<td>page 6-20</td>
</tr>
<tr>
<td>Reconfiguring Per-Port Values</td>
<td>Path Cost: Depends on port type Priority: 8 Edge Port: Yes Point-to-point: Force-true MCheck: Yes</td>
<td>page 6-18</td>
<td>page 6-16</td>
<td>—</td>
</tr>
<tr>
<td><strong>802.1s Spanning Tree Protocol</strong></td>
<td><strong>Default</strong></td>
<td><strong>Menu</strong></td>
<td><strong>CLI</strong></td>
<td><strong>Web</strong></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------</td>
<td>----------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Viewing the MSTP Status and Configuration</td>
<td>n/a</td>
<td>—</td>
<td>page 6-71</td>
<td>—</td>
</tr>
<tr>
<td>Enable/Disable MSTP and Configure Global Parameters</td>
<td>Disabled</td>
<td>—</td>
<td>page 6-57</td>
<td>—</td>
</tr>
<tr>
<td>Configuring Basic Port Connectivity Parameters</td>
<td>edge-port: No mcheck: Yes hello-time: 2 path-cost: auto point-to-point MAC: Force-True priority: 128 (multiplier: 8)</td>
<td>—</td>
<td>page 6-61 and following</td>
<td>—</td>
</tr>
<tr>
<td>Configuring MSTP Instance Parameters</td>
<td>instance (MSTPI): none priority: 32768 (multiplier: 8)</td>
<td>—</td>
<td>page 6-63</td>
<td>—</td>
</tr>
<tr>
<td>Configuring MSTP Instance Per-Port Parameters</td>
<td>Auto</td>
<td>—</td>
<td>page 6-66</td>
<td>—</td>
</tr>
<tr>
<td>Enabling/Disabling MSTP Spanning Tree Operation</td>
<td>Disabled</td>
<td>—</td>
<td>page 6-69</td>
<td>—</td>
</tr>
<tr>
<td>Enabling an Entire MST Region at Once</td>
<td>n/a</td>
<td>—</td>
<td>page 6-69</td>
<td>—</td>
</tr>
</tbody>
</table>

Without spanning tree, having more than one active path between a pair of nodes causes loops in the network, which can result in duplication of messages, leading to a “broadcast storm” that can bring down the network.

*Single-Instance spanning tree operation* (802.1D STP and 802.1w RSTP) ensures that only one active path at a time exists between any two nodes in a physical network. In networks where there is more than one physical, active path between any two nodes, enabling single-instance spanning tree ensures one active path between such nodes by blocking all redundant paths.

*Multiple-Instance spanning tree operation* (802.1s) ensures that only one active path exists between any two nodes in a spanning-tree *instance*. A spanning-tree instance comprises a unique set of VLANs, and belongs to a specific spanning-tree *region*. A region can comprise multiple spanning-tree instances (each with a different set of VLANs), and allows one active path among regions in a network. Applying VLAN tagging to the ports in a multiple-instance spanning-tree network enables blocking of redundant links in one instance while allowing forwarding over the same links for non-redundant use by another instance. For example, suppose you have three switches in a region...
configured with VLANs grouped into two instances, as follows:

<table>
<thead>
<tr>
<th>VLANs</th>
<th>Instance 1</th>
<th>Instance 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>10, 11, 12</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>20, 21, 22</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The logical and physical topologies resulting from these VLAN/Instance groupings result in blocking on different links for different VLANs:

Figure 6-1. Example of a Multiple Spanning-Tree Application
You should enable spanning tree operation in any switch that is part of a redundant physical link (loop topology). (HP recommends that you do so on all switches belonging to a loop topology.) This topic is covered in more detail under “How STP and RSTP Operate” on page 6-7.

As recommended in the IEEE 802.1Q VLAN standard, the Series 5300XL switches use single-instance STP for 802.1D and 802.1w spanning-tree operation. (In this case, the switch generates untagged Bridge Protocol Data Units—BPDUs.) This implementation creates a single spanning tree to make sure there are no network loops associated with any of the connections to the switch, regardless of whether multiple VLANs are configured on the switch. Thus, when using 802.1D or 802.1w spanning tree, these switches do not distinguish between VLANs when identifying redundant physical links. In this case, if VLANs are configured on the switch, see “STP Operation with 802.1Q VLANs” on page “RSTP and STP Operation with 802.1Q VLANs” on page 6-7.

The RSTP (802.1w) and STP (802.1D) Spanning Tree Options

Spanning tree interprets a switch mesh as a single link. Because the switch automatically gives faster links a higher priority, the default STP or RSTP parameter settings are usually adequate for spanning tree operation. Also, because incorrect STP or RSTP settings can adversely affect network performance, you should not make changes unless you have a strong understanding of how spanning tree operates.

In a mesh environment, the default RSTP timer settings (Hello Time and Forward Delay) are usually adequate for RSTP operation. Because a packet crossing a mesh may traverse several links within the mesh, using smaller-than-default settings for the RSTP Hello Time and Forward Delay timers can cause unnecessary topology changes and end-node connectivity problems.

For more on STP and RSTP, see the IEEE 802.1D and 802.1w standards.
RSTP (802.1w)

The IEEE 802.1D version of spanning tree (STP) can take a fairly long time to resolve all the possible paths and to select the most efficient path through the network. The IEEE 802.1w Rapid Reconfiguration Spanning Tree (RSTP) significantly reduces the amount of time it takes to establish the network path. The result is reduced network downtime and improved network robustness.

In addition to faster network reconfiguration, RSTP also implements greater ranges for port path costs to accommodate the higher and higher connection speeds that are being implemented.

RSTP is designed to be compatible with IEEE 802.1D STP, and HP recommends that you employ it in your network. For more information, refer to “Transitioning from STP to RSTP” on page 6-10.

STP (802.1D)

The IEEE 802.1D version of spanning tree has been in wide use and can coexist in a network in which RSTP (802.1w) has been introduced. If your network currently uses 802.1D STP and you are not yet ready to implement RSTP, you can apply STP to the Series 5300XL switches until such time as you are ready to move ahead with RSTP. STP on the Series 5300XL switches offers the full range of STP features found in earlier product releases, including:

- **STP Fast Mode for Overcoming Server Access Failures:** If an end node is configured to automatically access a server, the duration of the STP startup sequence can result in a “server access failure”. On ports where this is a problem, configuring STP Fast Mode can eliminate the failure. For more information, see “STP Fast Mode” on page 6-28. The next sections describe how to configure STP on the switch. For more information on STP operation, see “How STP and RSTP Operate” on page 6-7.

- **Fast-Uplink STP for Improving the Recovery (Convergence) Time in Wiring Closet Switches with Redundant Uplinks:** This means that a Series 5300XL switch having redundant links toward the root device can decrease the convergence time to a new uplink port to as little as ten seconds. For more information, refer to “Fast-Uplink Spanning Tree Protocol (STP)” on page 6-29.
How STP and RSTP Operate

The switch automatically senses port identity and type, and automatically defines spanning-tree parameters for each type, as well as parameters that apply across the switch. You can use the default values for these parameters, or adjust them as needed.

While allowing only one active path through a network at any time, spanning tree retains any redundant physical path to serve as a backup (blocked) path in case the existing active path fails. Thus, if an active path fails, spanning tree automatically activates (unblocks) an available backup to serve as the new active path for as long as the original active path is down. For example:

![Figure 6-2. General Example of Redundant Paths Between Two Nodes](image)

1. Active path from node A to node B: 1 —> 3
2. Backup (redundant) path from node A to node B: 4 —> 2 —> 3

In the factory default configuration, spanning tree operation is off. If a redundant link (loop) exists between nodes in your network, you should enable the spanning tree operation of your choice.

**Note**

Spanning tree retains its current parameter settings when disabled. Thus, if you disable spanning tree, then later re-enable it, the parameter settings will be the same as before spanning tree was disabled.

**RSTP and STP Operation with 802.1Q VLANs.** As recommended in the IEEE 802.1Q VLAN standard, when 802.1D or 802.1w spanning tree is enabled on the switch, a single spanning tree is configured for all ports across the switch, including those in separate VLANs. This means that if redundant physical links exist in separate VLANs, spanning tree will block all but one of those links. However, if you need to use spanning tree on the Series 5300XL switches in a VLAN environment with redundant physical links, you can
Spanning-Tree Operation
The RSTP (802.1w) and STP (802.1D) Spanning Tree Options

prevent blocked redundant links by using a port trunk. The following example
shows how you can use a port trunk with 802.1Q (tagged) VLANs and spanning
tree without unnecessarily blocking any links or losing any bandwidth.

Figure 6-3. Example of Using a Trunked Link with STP and VLANs
Configuring Rapid Reconfiguration Spanning Tree (RSTP)

This section describes the operation of the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP).

Overview

<table>
<thead>
<tr>
<th>RSTP Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing the RSTP/STP configuration</td>
<td>n/a</td>
<td>page 6-18</td>
<td>page 6-12</td>
<td>n/a</td>
</tr>
<tr>
<td>enable/disable RSTP/STP (RSTP is selected as the default protocol)</td>
<td>disabled</td>
<td>page 6-18</td>
<td>6-13</td>
<td>page 6-20</td>
</tr>
<tr>
<td>reconfiguring whole-switch values</td>
<td>Protocol Version: RSTP</td>
<td>page 6-18</td>
<td>page 6-14</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>Force Version: RSTP-operation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Switch Priority: 8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hello Time: 2 s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Max Age: 20 s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Forward Delay: 15 s</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reconfiguring per-port values</td>
<td>Path Cost: depends on port type</td>
<td>page 6-18</td>
<td>page 6-16</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td>Priority: 8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edge Port: Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Point-to-point: Force-true</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MCheck: Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As indicated in the manual, the spanning tree protocol is used to ensure that only one active path at a time exists between any two end nodes in the network in which your switch is installed. Multiple paths cause a loop in the network over which broadcast and multicast messages are repeated continuously, which floods the network with traffic creating a broadcast storm.

In networks where there is more than one physical path between any two nodes, enabling spanning tree ensures a single active path between two such nodes by selecting the one most efficient path and blocking the other redundant paths. If a switch or bridge in the path becomes disabled, spanning tree activates the necessary blocked segments to create the next most efficient path.
Transitioning from STP to RSTP

IEEE 802.1w RSTP is designed to be compatible with IEEE 802.1D STP. Even if all the other devices in your network are using STP, you can enable RSTP on your switch, and even using the default configuration values, your switch will interoperate effectively with the STP devices. If any of the switch ports are connected to switches or bridges on your network that do not support RSTP, RSTP can still be used on this switch. RSTP automatically detects when the switch ports are connected to non-RSTP devices in the spanning tree and communicates with those devices using 802.1D STP BPDU packets.

Because RSTP is so much more efficient at establishing the network path, though, that it is highly recommended that all your network devices be updated to support RSTP. RSTP offers convergence times of less than one second under optimal circumstances. To make the best use of RSTP and achieve the fastest possible convergence times, though, there are some changes that you should make to the RSTP default configuration. See “Optimizing the RSTP Configuration” below, for more information on these changes.

Note

Under some circumstances, it is possible for the rapid state transitions employed by RSTP to result in an increase in the rates of frame duplication and misordering in the switched LAN. In order to allow RSTP switches to support applications and protocols that may be sensitive to frame duplication and misordering, setting the Force Protocol Version parameter to stp-compatible allows RSTP to be operated with the rapid transitions disabled. The value of this parameter applies to all ports on the switch. See the information on Force Version on page 6-14.

As indicated above, one of the benefits of RSTP is the implementation of a larger range of port path costs, which accommodates higher network speeds. New default values have also been implemented for the path costs associated with the different network speeds. This can create some incompatibility between devices running the older 802.1D STP and your switch running RSTP. Please see the “Note on Path Cost” on page 6-17 for more information on adjusting to this incompatibility.
Configuring RSTP

The default switch configuration has spanning tree disabled with RSTP as the selected protocol. That is, when spanning tree is enabled, RSTP is the version of spanning tree that is enabled, by default.

Optimizing the RSTP Configuration

To optimize the RSTP configuration on your switch, follow these steps (note that for the Menu method, all of these steps can be performed at the same time by making all the necessary edits on the “Spanning Tree Operation” screen and then saving the configuration changes):

1. Set the switch to support RSTP (RSTP is the default):
   - **CLI:** `spanning-tree protocol-version rstp`
   - **Menu:** Main Menu —> 2. Switch Configuration —> 4. Spanning Tree Operation —> select Protocol Version: RSTP

2. Set the “point-to-point-mac” value to false on all ports that are connected to shared LAN segments (that is, to connections to hubs):
   - **CLI:** `spanning-tree [ethernet] <port-list> point-to-point-mac force-false`
   - **Menu:** Main Menu —> 2. Switch Configuration —> 4. Spanning Tree Operation —> for each appropriate port, select Point-to-Point: Force-False

3. Set the “edge-port” value to false for all ports connected to other switches, bridges, and hubs:
   - **CLI:** `no spanning-tree [ethernet] <port-list> edge-port`
   - **Menu:** Main Menu —> 2. Switch Configuration —> 4. Spanning Tree Operation —> for each appropriate port, select Edge: No

4. Set the “mcheck” value to false for all ports that are connected to devices that are known to be running IEEE 802.1D spanning tree:
   - **CLI:** `no spanning-tree [ethernet] <port-list> mcheck`
   - **Menu:** Main Menu —> 2. Switch Configuration —> 4. Spanning Tree Operation —> for each appropriate port, select MCheck: No

5. Enable RSTP Spanning Tree:
   - **CLI:** `spanning-tree`
   - **Menu:** Main Menu —> 2. Switch Configuration —> 4. Spanning Tree Operation —> select STP Enabled: Yes
CLI: Configuring RSTP

<table>
<thead>
<tr>
<th>Spanning Tree Commands in This Section</th>
<th>STP</th>
<th>RSTP</th>
<th>Page for RSTP Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree config</td>
<td>Y</td>
<td>Y</td>
<td>Below on this page</td>
</tr>
<tr>
<td>spanning-tree</td>
<td>Y</td>
<td>Y</td>
<td>6-13</td>
</tr>
<tr>
<td>protocol-version &lt;rstp</td>
<td>stp&gt;</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>force-version &lt;rstp-operation</td>
<td>stp-compatible&gt;</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>forward-delay &lt;4 - 30&gt;</td>
<td>Y</td>
<td>Y</td>
<td>page 6-14</td>
</tr>
<tr>
<td>hello-time &lt;1 - 10&gt;</td>
<td>Y</td>
<td>Y</td>
<td>page 6-14</td>
</tr>
<tr>
<td>maximum-age &lt;6 - 40&gt;</td>
<td>Y</td>
<td>Y</td>
<td>page 6-14</td>
</tr>
<tr>
<td>priority &lt;0 - 15</td>
<td>0 - 65535&gt;</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>&lt;[ethernet] port-list&gt;</td>
<td>Y</td>
<td>Y</td>
<td>page 6-16</td>
</tr>
<tr>
<td>path-cost &lt;1 - 200 000 000&gt;</td>
<td>Y</td>
<td>Y</td>
<td>page 6-16</td>
</tr>
<tr>
<td>priority &lt;0 - 15</td>
<td>0 - 65535&gt;</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>edge-port</td>
<td>N</td>
<td>Y</td>
<td>page 6-16</td>
</tr>
<tr>
<td>point-to-point-mac</td>
<td>N</td>
<td>Y</td>
<td>page 6-16</td>
</tr>
<tr>
<td>mcheck</td>
<td>N</td>
<td>Y</td>
<td>page 6-16</td>
</tr>
<tr>
<td>mode &lt;norm</td>
<td>fast&gt;</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>

show spanning-tree

This command lists additional RSTP/STP/MSTP monitoring data that is not covered in this section. Refer to the section titled “Spanning Tree Protocol Information” in the “Monitoring and Analyzing Switch Operation” appendix of the Management and Configuration Guide for your switch.

Viewing the Current Spanning Tree Configuration. Use this command to display the current spanning tree configuration.

Syntax: show spanning-tree configuration

Lists the switch’s full spanning tree configuration, including whole-switch and per-port settings, regardless of whether spanning tree is disabled.

(Default: n/a; Abbreviated Command: sho span config)

In the default configuration, the output from this command appears similar to the following:
Figure 6-4. Example of the Spanning Tree Configuration Display

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Cost</th>
<th>Priority</th>
<th>Edge</th>
<th>Point-to-Point</th>
<th>MCheck</th>
<th>Hello Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A2 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A3 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>. . . . .</td>
<td>. . .</td>
<td>. . .</td>
<td>. . .</td>
<td>. . .</td>
<td>. . .</td>
<td>. . .</td>
</tr>
<tr>
<td>A21 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A22 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A23 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
<tr>
<td>A24 10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
<td>Use Global</td>
</tr>
</tbody>
</table>

Enabling or Disabling RSTP. Issuing the command to enable spanning tree on the switch implements, by default, the RSTP version of spanning tree for all physical ports on the switch. Disabling spanning tree removes protection against redundant network paths.

**Syntax:** [no] spanning-tree

**Abbreviation:** [no] span

This command enables spanning tree with the current parameter settings or disables spanning tree, using the “no” option, without losing the most-recently configured parameter settings.

Enabling STP Instead of RSTP. If you decide, for whatever reason, that you would prefer to run the IEEE 802.1D (STP) version of spanning tree, then issue the following command:

**Syntax:** spanning-tree protocol-version stp

**Abbreviation:** span prot stp

For the STP version of spanning tree, the rest of the information in this section does not apply. Refer to “802.1D Spanning-Tree Protocol (STP)” on page 6-21 for more information on the STP version and its parameters.
Reconfiguring Whole-Switch Spanning Tree Values. You can configure one or more of the following parameters, which affect the spanning tree operation of the whole switch:

Table 6-1. Whole-Switch RSTP Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol-version</td>
<td>RSTP</td>
<td>Identifies which of the spanning tree protocols will be used when spanning tree is enabled on the switch.</td>
</tr>
<tr>
<td>force-version</td>
<td>rstp-operation</td>
<td>Sets the spanning tree compatibility mode. Even if rstp-operation is selected though, if the switch detects STP BPDU packets on a port, it will communicate to the attached device using STP BPDU packets. If errors are encountered, as described in the Note on page 6-10, the Force-Version value can be set to stp-compatible, which forces the switch to communicate out all ports using operations that are compatible with IEEE 802.1D STP.</td>
</tr>
</tbody>
</table>
| priority         | 32768 (8 as a step value) | Specifies the protocol value used along with the switch MAC address to determine which device in the spanning tree is the root. The lower the priority value, the higher the priority.  
The value you enter has changed from the STP value. The range is 0 - 61440, but for RSTP the value is entered as a multiple (a step) of 4096. You enter a value in the range 0 - 15. The default value of 32768 is derived by the default setting of 8.  
Displaying the RSTP configuration (show spanning-tree config) shows 8, but displaying the RSTP operation (show spanning-tree) shows 32768. |
| maximum-age      | 20 seconds    | Sets the maximum age of received spanning tree information before it is discarded. The range is 6 to 40 seconds.                              |
| hello-time       | 2 seconds     | Sets the time between transmission of spanning tree messages. Used only when this switch is the root. The range is 1 to 10 seconds.            |
| forward-delay    | 15 seconds    | Sets the time the switch waits between transitioning ports from listening to learning and from learning to forwarding states. The range is 4 to 30 seconds. |

*These parameters are the same for RSTP as they are for STP. The switch uses its own maximum-age, hello-time, and forward-delay settings only if it is operating as the root device in the spanning tree. If another device is the root device, then the switch uses the other device’s settings for these parameters.
Executing the **spanning-tree** command alone enables spanning tree. Executing the command with one or more of the whole-switch RSTP parameters shown in the table on the previous page, or with any of the per-port RSTP parameters shown in the table on page 6-16, does not enable spanning tree. It only configures the spanning tree parameters, regardless of whether spanning tree is actually running (enabled) on the switch.

Using this facility, you can completely configure spanning tree the way you want and then enable it. This method minimizes the impact on the network operation.

**Syntax:**

<table>
<thead>
<tr>
<th>Command</th>
<th>Abbreviations</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree protocol-version &lt;rstp</td>
<td>span prot &lt;rstp</td>
</tr>
<tr>
<td></td>
<td>forc &lt;rstp</td>
</tr>
<tr>
<td></td>
<td>pri &lt;0 - 15&gt;</td>
</tr>
<tr>
<td></td>
<td>hello &lt;1 - 10&gt;</td>
</tr>
<tr>
<td></td>
<td>forward-delay &lt;4 - 30 seconds&gt;</td>
</tr>
</tbody>
</table>

**Defaults:** See the table on the previous page.

Multiple parameters can be included on the same command line. For example, to configure a maximum-age of 30 seconds and a hello-time of 3 seconds, you would issue the following command:

```
HPswitch (config)# span max 30 hello 3
```
Reconfiguring Per-Port Spanning Tree Values. You can configure one or more of the following parameters, which affect the spanning tree operation of the specified ports only:

**Table 6-2. Per-Port RSTP Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>edge-port</td>
<td>Yes</td>
<td>Identifies ports that are connected to end nodes. During spanning tree establishment, these ports transition immediately to the Forwarding state. In this way, the ports operate very similarly to ports that are configured in &quot;fast mode&quot; under the STP implementation in previous HP switch software. Disable this feature on all switch ports that are connected to another switch, or bridge, or hub. Use the “no” option on the spanning tree command to disable edge-port. This option is available only with RSTP or MSTP operation. (Note that when MSTP is enabled, the edge-port default setting is disabled.)</td>
</tr>
<tr>
<td>mcheck</td>
<td>Yes</td>
<td>Ports with mcheck set to true are forced to send out RSTP BPDUs for 3 seconds. This allows for switches that are running RSTP to establish their connection quickly and for switches running 802.1D STP to be identified. If the whole-switch parameter Force-Version is set to “stp-compatible”, the mcheck setting is ignored and STP BPDUs are sent out all ports. Disable this feature on all ports that are known to be connected to devices that are running 802.1D STP. Use the “no” option on the spanning tree command to disable mcheck. This option is available only with RSTP or MSTP operation.</td>
</tr>
<tr>
<td>path-cost</td>
<td>10 Mbps – 2 000 000 100 Mbps – 200 000 1 Gbps – 20 000</td>
<td>Assigns an individual port cost that the switch uses to determine which ports are the forwarding ports. The range is 1 to 200,000,000 or auto. By default, this parameter is automatically determined by the port type, as shown by the different default values. If you have previously configured a specific value for this parameter, you can issue the command with the <strong>auto</strong> option to restore the automatic setting feature. Please see the Note on Path Cost on page 6-17 for information on compatibility with devices running 802.1D STP for the path cost values.</td>
</tr>
<tr>
<td>point-to-</td>
<td>force-true</td>
<td>This parameter is used to tell the port if it is connected to a point-to-point link, such as to another switch or bridge or to an end node (force-true). This parameter should be set to force-false for all ports that are connected to a hub, which is a shared LAN segment. You can also set this parameter to auto and the switch will automatically set the force-false value on all ports that it detects are not running at full duplex. All connections to hubs are not full duplex. This command is available only with RSTP operation.</td>
</tr>
<tr>
<td>point-mac</td>
<td></td>
<td></td>
</tr>
<tr>
<td>priority</td>
<td>128 (8 as a step value)</td>
<td>This parameter is used by RSTP to determine the port(s) to use for forwarding. The port with the lowest number has the highest priority. The range is 0 to 240, but you configure the value by entering a multiple of 16. You enter a value in the range 0 - 15. The default value of 128 is derived by the default setting of 8. Displaying the RSTP configuration (<strong>show spanning-tree config</strong>) shows 8, but displaying the RSTP operation (<strong>show spanning-tree</strong>) shows 128.</td>
</tr>
</tbody>
</table>
Spanning-Tree Operation
Configuring Rapid Reconfiguration Spanning Tree (RSTP)

Syntax:

```
spanning-tree [ethernet] <port-list>
  path-cost < 1 - 200000000 >
  point-to-point-mac < force-true | force-false | auto >
  priority < 0 - 15 >
[no] spanning-tree [ethernet] <port-list>
  edge-port
  mcheck
```

Abbreviations:

```
span < port-list >
  path < 1 - 200000000 >
  forc < force-t | force-f | auto >
  pri < 0 - 15 >
[no] span < port-list >
  edge
  mch
```

Defaults: see the table on the previous page.

**Note on Path Cost**

RSTP and MSTP implement a greater range of path costs and new default path cost values to account for higher network speeds. These values are different than the values defined by 802.1D STP as shown below.

<table>
<thead>
<tr>
<th>Port Type</th>
<th>802.1D STP Path Cost</th>
<th>RSTP and MSTP Path Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Mbps</td>
<td>100</td>
<td>2000000</td>
</tr>
<tr>
<td>100 Mbps</td>
<td>10</td>
<td>200000</td>
</tr>
<tr>
<td>1 Gbps</td>
<td>5</td>
<td>20000</td>
</tr>
</tbody>
</table>

Because the maximum value for the path cost allowed by 802.1D STP is 65535, devices running that version of spanning tree cannot be configured to match the values defined by RSTP and MSTP, at least for 10 Mbps and 100 Mbps ports. In LANs where there is a mix of devices running 802.1D STP, RSTP, and/or MSTP, you should reconfigure the devices so the path costs match for ports with the same network speeds.
Spanning-Tree Operation
Configuring Rapid Reconfiguration Spanning Tree (RSTP)

Menu: Configuring RSTP

1. From the console CLI prompt, enter the menu command.
   
   HP Procurve Switch # menu

2. From the switch console Main Menu, select
   2. Switch Configuration …
     4. Spanning Tree Operation


4. Press the Space bar to select the version of spanning tree you wish to run: RSTP or STP.

   Note: If you change the protocol version, you will have to reboot the switch for the change to take effect. See step 9 and step 10.

5. Press the [Tab] or down arrow key to go to the STP Enabled field. Note that when you do this, the remaining fields on the screen will then be appropriate for the version of spanning tree that was selected in step 3. The screen image below is for RSTP.

6. Press the Space bar to select Yes to enable spanning tree.
7. Press the [Tab] key or use the arrow keys to go to the next parameter you want to change, then type in the new value or press the Space bar to select a value. (To get help on this screen, press [Enter] to select the Actions –> line, then press [H], for Help, to display the online help.)

8. Repeat step 6 for each additional parameter you want to change.

   Please see “Optimizing the RSTP Configuration” on page 6-11 for recommendations on configuring RSTP to make it operate the most efficiently.

9. When you are finished editing parameters, press [Enter] to return to the Actions –> line and press [S] to save the currently displayed spanning tree settings and return to the Main Menu.

10. If you have changed the Protocol Version, in step 1, reboot the switch now by selecting

   6. Reboot Switch
Web: Enabling or Disabling RSTP

In the web browser interface, you can enable or disable spanning tree on the switch. If the default configuration is in effect such that RSTP is the selected protocol version, enabling spanning tree through the web browser interface will enable RSTP with its current configuration. To configure the other spanning tree features, telnet to the switch console and use the CLI or menu.

To enable or disable spanning tree using the web browser interface:

1. Click on the **Configuration** tab.
2. Click on **Device Features**.
3. Enable or disable spanning tree.
4. Click on **Apply Changes** to implement the configuration change.
802.1D Spanning-Tree Protocol (STP)

Menu: Configuring 802.1D STP

1. From the Main Menu, select:
   
   2. Switch Configuration …

   4. Spanning Tree Operation

---

**Figure 6-6. The Default “Spanning Tree Operation” Screen**

2. Press [E] (for Edit) to highlight the **Protocol Version** field. In the default configuration this field is set to **RSTP**.

3. Press the Space bar once to change the field to STP. This changes the Protocol Version selection to the 802.1D Spanning Tree Protocol.

4. Press [↑] to highlight the **STP Enabled** field.

5. Press the Space bar to select **Yes**. (Yes in this field means to enable spanning-tree operation.)
Spanning-Tree Operation
802.1D Spanning-Tree Protocol (STP)

6. If the remaining STP parameter settings are adequate for your network, go to step 10.

7. Use [Tab] or the arrow keys to select the next parameter you want to change, then type in the new value or press the Space Bar to select a value. (If you need information on STP parameters, press [Enter] to select the Actions line, then press H to get help.)

8. Repeat step 7 for each additional parameter you want to change.

Note: For information on the Mode parameter, see “STP Fast Mode” on page 6-28.

9. When you are finished editing parameters, press [Enter] to return to the Actions line.

10. Press [S] to save the currently displayed STP parameter settings. You will then see the “Switch Configuration Menu” with an asterisk (*) at the Spanning Tree Operation line, indicating that you must reboot the switch before the Protocol Version change (step 5) takes effect.

Figure 6-7. Enabling Spanning-Tree Operation
Spanning-Tree Operation

802.1D Spanning-Tree Protocol (STP)

Figure 6-8. The Configuration Menu Indicating a Reboot Is Needed to Implement a Configuration Change

11. Press [0] to return to the Main menu.

Figure 6-9. The Main Menu Indicating a Reboot Is Needed To Implement a Configuration Change

CLI: Configuring 802.1D STP

STP Commands Used in This Section

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show spanning-tree config</td>
<td>6-25</td>
</tr>
<tr>
<td>spanning-tree</td>
<td></td>
</tr>
<tr>
<td>protocol-version</td>
<td>6-25</td>
</tr>
<tr>
<td>forward-delay</td>
<td>6-26</td>
</tr>
<tr>
<td>hello-time</td>
<td>6-26</td>
</tr>
<tr>
<td>maximum-age</td>
<td>6-26</td>
</tr>
<tr>
<td>priority</td>
<td>6-26</td>
</tr>
<tr>
<td>ethernet</td>
<td>6-27</td>
</tr>
<tr>
<td>path-cost</td>
<td>6-27</td>
</tr>
<tr>
<td>priority</td>
<td>6-27</td>
</tr>
<tr>
<td>mode</td>
<td>6-27</td>
</tr>
</tbody>
</table>

Viewing the Current STP Configuration.

**Syntax:** show spanning-tree config

Regardless of whether STP is disabled (the default), this command lists the switch’s full STP configuration, including general settings and port settings.

When the switch is configured for 802.1D STP, this command displays information similar to the following:

```
HPswitch(config)# show spanning-tree config
Spanning Tree Operation

Protocol Version : STP
STP Enabled [No] : No
Switch Priority [32768] : 32768
Max Age [20] : 20
Forward Delay [15] : 15

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Cost</th>
<th>Priority</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Norm</td>
</tr>
<tr>
<td>A2</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Norm</td>
</tr>
<tr>
<td>A3</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Norm</td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Norm</td>
</tr>
<tr>
<td>A5</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Norm</td>
</tr>
</tbody>
</table>

Figure 6-10. Example of the Default STP Configuration Listing with 802.1D STP Configured at the Protocol Version
Configuring the Switch To Use the 802.1D Spanning Tree Protocol (STP). In the default configuration, the switch is set to RSTP (that is, 802.1w Rapid Spanning Tree), and spanning tree operation is disabled. To reconfigure the switch to 802.1D spanning tree, you must:

1. Change the spanning tree protocol version to stp.
2. Use write memory to save the change to the startup-configuration.
3. Reboot the switch.
4. If you have not previously enabled spanning-tree operation on the switch, use the spanning-tree command again to enable STP operation.

**Syntax:**
```
spanning-tree protocol-version stp
write memory
boot
```

For example:

```
HPswitch(config)# spanning-tree protocol-version stp
STP version was changed. To activate the change you must save the configuration to flash and reboot the device.
HPswitch(config)# write memory
HPswitch(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

**Figure 6-11. Steps for Changing Spanning-Tree Operation to the 802.1D Protocol**

Enabling (or Disabling) Spanning Tree Operation on the Switch.

**Syntax:** `[no] spanning-tree

This command enables (or disables) spanning tree operation for either spanning tree version—STP/802.1D or RSTP/802.1w (the default). (Default: Disabled.)

Before using this command, ensure that the version of spanning tree you want to use is active on the switch. (See the preceding topic, “Configuring the Switch To Use the 802.1D Spanning Tree Protocol (STP)” on page 6-25.)

For example:

```
HPswitch spanning-tree
```
Enabling STP implements the spanning tree protocol for all physical ports on the switch, regardless of whether multiple VLANs are configured. Disabling STP removes protection against redundant loops that can significantly slow or halt a network.

This command enables STP with the current parameter settings or disables STP without losing the most-recently configured parameter settings. (To learn how the switch handles parameter changes, how to test changes without losing the previous settings, and how to replace previous settings with new settings, refer to the chapter titled “Switch Memory and Configuration” in the Management and Configuration Guide for your switch.) When enabling STP, you can also include the STP general and per-port parameters described in the next two sections. When you use the “no” form of the command, you can do so only to disable STP. (STP parameter settings are not changed when you disable STP.)

Because incorrect STP settings can adversely affect network performance, HP recommends that you use the default STP parameter settings. You should not change these settings unless you have a strong understanding of how STP operates. For more on STP, see the IEEE 802.1D standard.

**Reconfiguring General STP Operation on the Switch.** You can configure one or more of the following parameters:

**Table 6-3. General STP Operating Parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Range</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>32768</td>
<td>0 - 65535</td>
<td>Specifies the priority value used along with the switch MAC address to determine which device is root. The lower a priority value, the higher the priority.</td>
</tr>
<tr>
<td>*maximum-age</td>
<td>20 seconds</td>
<td>6 - 40 seconds</td>
<td>Maximum received message age the switch allows for STP information before discarding the message.</td>
</tr>
<tr>
<td>*hello-time</td>
<td>2 seconds</td>
<td>1 - 10</td>
<td>Time between messages transmitted when the switch is the root.</td>
</tr>
<tr>
<td>*forward-delay</td>
<td>15 seconds</td>
<td>4 - 30 seconds</td>
<td>Time the switch waits before transitioning from the listening to the learning state, and between the learning state to the forwarding state.</td>
</tr>
</tbody>
</table>

*The switch uses its own maximum-age, hello-time, and forward-delay settings only if it is operating as the root device. If another device is operating as the root device, then the switch uses the other device’s settings for these parameters.
Note

Executing `spanning-tree` alone enables STP. Executing spanning-tree with one or more of the above “STP Operating Parameters” does not enable STP. It only configures the STP parameters (regardless of whether STP is actually running (enabled) on the switch).

Syntax: `spanning-tree`
- `priority < 0 - 65535>`
- `maximum-age < 6 - 40 seconds>`
- `hello-time < 1 - 10 seconds>`
- `forward-delay < 4 - 30 seconds>`

Default: Refer to table 6-3, above.

For example, to configure a `maximum-age` of 30 seconds and a `hello-time` of 3 seconds for STP:

```
HPswitch(config)# spanning-tree maximum-age 30 hello-time 3
```

Reconfiguring Per-Port STP Operation on the Switch.

Syntax: `spanning-tree < port-list > path-cost < 1 - 65535 > priority < 0 - 255 > mode < norm | fast >`

Enables STP (if not already enabled) and configures the per-port parameters listed in table 6-4.

Table 6-4. Per-Port STP Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Default</th>
<th>Range</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>path-cost</td>
<td>Ethernet: 100 10/100Tx: 10 100Fx: 10 Gigabit: 5</td>
<td>1 - 65535</td>
<td>Assigns an individual port cost that the switch uses to determine which ports are the forwarding ports.</td>
</tr>
<tr>
<td>priority</td>
<td>128</td>
<td>0 - 255</td>
<td>Used by STP to determine the port(s) to use for forwarding. The port with the lowest number has the highest priority.</td>
</tr>
<tr>
<td>mode</td>
<td>norm</td>
<td>norm - or - fast - or - uplink</td>
<td>Specifies whether a port progresses through the listening, learning, and forwarding (or blocking) states (“norm” mode) or transitions directly to the forwarding state (“fast” mode).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For information on when to use Fast mode, see “STP Fast Mode” on page 6-28.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• For information on Uplink mode, see “Fast-Uplink Spanning Tree Protocol (STP)” on page 6-29</td>
</tr>
</tbody>
</table>
You can also include STP general parameters in this command. See “Reconfiguring General STP Operation on the Switch” on page 6-26.

For example, the following configures ports C5 and C6 to a path cost of 15, a priority of 100, and fast mode:

```
HPswitch(config)# spanning-tree c5-c6 path-cost 15 priority 100 mode fast
```

**STP Fast Mode**

For standard STP operation, when a network connection is established on a device that is running STP, the port used for the connection goes through a sequence of states (Listening and Learning) before getting to its final state (Forwarding or Blocking, as determined by the STP negotiation). This sequence takes two times the forward delay value configured for the switch. The default is 15 seconds on HP switches, per the IEEE 802.1D standard recommendation, resulting in a total STP negotiation time of 30 seconds. Each switch port goes through this start-up sequence whenever the network connection is established on the port. This includes, for example, when the switch or connected device is powered up, or the network cable is connected.

A problem can arise from this long STP start-up sequence because some end nodes are configured to automatically try to access a network server whenever the end node detects a network connection. Typical server access includes to Novell servers, DHCP servers, and X terminal servers. If the server access is attempted during the time that the switch port is negotiating its STP state, the server access will fail. To provide support for this end node behavior, the Series 5300XL switches offers a configuration mode, called “Fast Mode”, that causes the switch port to skip the standard STP start-up sequence and put the port directly into the “Forwarding” state, thus allowing the server access request to be forwarded when the end node needs it.

If you encounter end nodes that repeatedly indicate server access failure when attempting to bring up their network connection, and you have enabled STP on the switch, try changing the configuration of the switch ports associated with those end nodes to STP Fast Mode.

---

**Caution**

The Fast Mode configuration should be used only on switch ports connected to end nodes. Changing the Mode to Fast on ports connected to hubs, switches, or routers may cause loops in your network that STP may not be able to immediately detect, in all cases. This will cause temporary loops in your network. After the fast start-up sequence, though, the switch ports operate according to the STP standard, and will adjust their state to eliminate continuing network loops.
To Enable or Disable Fast Mode for a Switch Port: You can use either the CLI or the menu interface to toggle between STP Fast mode and STP Normal mode. (To use the menu interface, see “Menu: Configuring 802.1D STP” on page 6-21.)

Syntax: spanning-tree < port-list > mode <fast | norm>

For example, to configure Fast mode for ports C1-C3 and C5:

HPswitch(config)# spanning-tree c1-c3,c5 mode fast

Fast-Uplink Spanning Tree Protocol (STP)

Fast-Uplink STP is an option added to the switch’s 802.1D STP to improve the recovery (convergence) time in wiring closet switches with redundant uplinks. Specifically, a Series 5300XL switch having redundant links toward the root device can decrease the convergence time (or failover) to a new uplink (STP root) port to as little as ten seconds. To realize this performance, the switch must be:

- Used as a wiring closet switch (also termed an edge switch or a leaf switch).
- Configured for fast-uplink STP mode on two or more ports intended for redundancy in the direction of the root switch, so that at any time only one of the redundant ports is expected to be in the forwarding state.

Note

Fast-Uplink STP operates only with 802.1D STP and is not available with the Rapid STP (802.1w) feature (6-9).
In general, fast-uplink spanning tree on the Series 5300XL switches is useful when running STP in a tiered topology that has well-defined edge switches. Also, ensure that an interior switch is used for the root switch and for any logical backup root switches. You can accomplish this by using the Spanning Tree Priority (sometimes termed bridge priority) settings that define the primary STP root switch and at least one failover root switch (in the event that the primary root switch fails). Inappropriate use of Fast-Uplink STP can cause intermittent loops in a network topology. For this reason, the Fast-Uplink STP feature should be used only by experienced network administrators who have a strong understanding of the IEEE 802.1D standard and STP interactions and operation. If you want to learn more about STP operation, you may find it helpful to refer to publications such as:


When properly implemented, fast-uplink STP offers a method for achieving faster failover times than standard STP, and is intended for this purpose for instances where 802.1D STP has been chosen over 802.1w RSTP.

To use fast-uplink STP, configure fast-uplink (Mode = Uplink) only on the switch’s upstream ports; (that is, two or more ports forming a group of redundant links in the direction of the STP root switch). If the active link in this group goes down, fast-uplink STP selects a different upstream port as the root port and resumes moving traffic in as little as ten seconds. The device(s) on the other end of the links must be running STP. However, because fast uplink should be configured only on the Series 5300XL switch uplink ports, the device(s) on the other end of the links can be either HP devices or another vendor’s devices, regardless of whether they support fast uplink. For example:

![Diagram of how to implement Fast-Uplink STP](image)

**Figure 6-12. Example of How To Implement Fast-Uplink STP**
### Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>downlink port (downstream port)</td>
<td>A switch port that is linked to a port on another switch (or to an end node) that is sequentially further away from the STP root device. For example, port “C” in figure 6-12, above, is a downlink port.</td>
</tr>
<tr>
<td>edge switch</td>
<td>For the purposes of fast-uplink STP, this is a switch that has no other switches connected to its downlink ports. An edge switch is sequentially further from the root device than other switches to which it is connected. Also termed wiring closet switch or leaf switch. For example, switch “4” in figure 6-13 (page 6-31) is an edge switch.</td>
</tr>
<tr>
<td>interior switch</td>
<td>In an STP environment, a switch that is sequentially closer to the STP root device than one or more other switches to which it is connected. For example, switches “1”, “2”, and “3” in figure 6-13 (page 6-31) are interior switches.</td>
</tr>
<tr>
<td>single-instance spanning tree</td>
<td>A single spanning-tree ensuring that there are no logical network loops associated with any of the connections to the switch, regardless of whether there are any VLANs configured on the switch. For more information, see “Spanning Tree Protocol (STP)” in chapter 9, “Configuring Advanced Features”, in the Management and Configuration Guide for your switch.</td>
</tr>
<tr>
<td>uplink port (upstream port)</td>
<td>A switch port linked to a port on another switch that is sequentially closer to the STP root device. For example, ports “A” and “B” in figure 6-12 on page 6-30 are uplink ports.</td>
</tr>
<tr>
<td>wiring closet switch</td>
<td>Another term for an “edge” or “leaf” switch.</td>
</tr>
</tbody>
</table>

When single-instance spanning tree (STP) is running in a network and a forwarding port goes down, a blocked port typically requires a period of

$$(2 \times \text{forward delay}) + \text{link down detection}$$


to transition to forwarding. In a normal spanning tree environment, this transition is usually 30 seconds (with the Forward Delay parameter set to its default of 15 seconds). However, by using the fast-uplink spanning tree feature, a port on a Series 5300XL switch used as an edge switch can make this transition in as little as ten seconds. (In an STP environment, an edge switch is a switch that is connected only to switches that are closer to the STP root switch than the edge switch itself, as shown by switch “4” in figure 6-13, below.)

![Diagram of an Edge Switch](image)

**Figure 6-13. Example of an Edge Switch in a Topology Configured for STP Fast Uplink**
In figure 6-13, STP is enabled and in its default configuration on all switches, unless otherwise indicated in table 6-5, below:

**Table 6-5. STP Parameter Settings for Figure 6-13**

<table>
<thead>
<tr>
<th>STP Parameter</th>
<th>Switch &quot;1&quot;</th>
<th>Switch &quot;2&quot;</th>
<th>Switch &quot;3&quot;</th>
<th>Switch &quot;4&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Priority</td>
<td>0(^1)</td>
<td>1(^2)</td>
<td>32,768 (default)</td>
<td>32,768 (default)</td>
</tr>
<tr>
<td>(Fast) Uplink</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Ports 3 &amp; 5</td>
</tr>
</tbody>
</table>

\(^1\) This setting ensures that Switch "1" will be the primary root switch for STP in figure 6-13.

\(^2\) This setting ensures that Switch "2" will be the backup root switch for STP in figure 6-13.

With the above-indicated topology and configuration:

- **Scenario 1:** If the link between switches “4” and “2” goes down, then the link between switches “4” and “3” will begin forwarding in as little as ten seconds.

- **Scenario 2:** If Switch “1” fails, then:
  - Switch “2” becomes the root switch.
  - The link between Switch “3” and Switch “2” begins forwarding.
  - The link between Switch “2” and the LAN begins forwarding.

**Operating Rules for Fast Uplink**

- A switch with ports configured for fast uplink must be an edge switch and not either an interior switch or the STP root switch.

  Configure fast-uplink on only the edge switch ports used for providing redundant STP uplink connections in a network. (Configuring Fast-Uplink STP on ports in interior switches can create network performance problems.) That is, a port configured for STP uplink should not be connected to a switch that is sequentially further away from the STP root device. For example, switch “4” in figure 6-13 (page 6-31) is an edge switch.

- Configure fast uplink on a group (two or more) of redundant edge-switch uplink ports where only one port in the group is expected to be in the forwarding state at any given time.
Edge switches cannot be directly linked together using fast-uplink ports. For example, the connection between switches 4 and 5 in figure 6-14 is not allowed for fast-uplink operation.

The ports that make up this link cannot be configured as fast-uplink ports.

Figure 6-14. Example of a Disallowed Connection Between Edge Switches

- Apply fast-uplink only on the uplink ports of an edge switch. For example, on switch “4” (an edge switch) in figure 6-14 above, only the ports connecting switch “4” to switches “2” and “3” are upstream ports that would use fast uplink. Note also that fast uplink should not be configured on both ends of a point-to-point link, but only on the uplink port of an edge switch.

- Ensure that the switch you intend as a backup root device will in fact become the root if the primary root fails, and that no ports on the backup root device are configured for fast-uplink operation. For example, if the **STP Priority** is the same on all switches—default: 32768—then the switch with the lowest MAC address will become the root switch. If that switch fails, then the switch with the next-lowest MAC address will become the root switch. Thus, you can use **STP Priority** to control which switch STP selects as the root switch and which switch will become the root if the first switch fails.

- Fast-Uplink STP requires a minimum of two uplink ports.

Menu: Viewing and Configuring Fast-Uplink STP

You can use the menu to quickly display the entire STP configuration and to make any STP configuration changes.
To View and/or Configure Fast-Uplink STP. This procedure uses the Spanning Tree Operation screen to enable STP and to set the Mode for fast-uplink STP operation.

1. From the Main Menu select:
   2. Switch Configuration …
   4. Spanning Tree Operation

2. In the default STP configuration, RSTP is the selected protocol version. If this is the case on your switch, you must change the Protocol Version to STP in order to use Fast-Uplink STP:

```
------------------------ CONSOLE - MANAGER MODE ------------------------

Switch Configuration - Spanning Tree Operation

Protocol Version: (RSTP)
STP Enabled [No] : No
Force Version [RSTP-operation] : RSTP-operation

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Cost</th>
<th>Priority</th>
<th>Edge</th>
<th>Point-to-Point</th>
<th>MCheck</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3</td>
<td>10/100TX</td>
<td>200000</td>
<td>8</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
<td>200000</td>
<td>8</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
</tr>
<tr>
<td>A5</td>
<td>10/100TX</td>
<td>200000</td>
<td>8</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
</tr>
<tr>
<td>A6</td>
<td>10/100TX</td>
<td>200000</td>
<td>8</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
</tr>
<tr>
<td>A7</td>
<td>10/100TX</td>
<td>200000</td>
<td>8</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
</tr>
<tr>
<td>A8</td>
<td>10/100TX</td>
<td>200000</td>
<td>8</td>
<td>Yes</td>
<td>Force-True</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Actions->  Cancel  Edit  Save  Help
```

Figure 6-15. The Default STP Screen With the Protocol Version Field Set to “RSTP”
3. If the Protocol Version is set to RSTP (as shown in figure 6-15), do the following:
   a. Press [E] (Edit) to move the cursor to the Protocol Version field.
   b. Press the Space bar once to change the Protocol Version field to STP.
   c. Press [Enter] to return to the command line.
   d. Press [S] (for Save) to save the change and exit from the Spanning Tree Operation screen. you will then see a screen with the following:

   Figure 6-16. Changing from RSTP to STP Requires a System Reboot

   e. Press [0] (zero) to return to the Main Menu, then [6] to reboot the switch.

   f. After you reboot the switch, enter the menu command at the CLI to return to the Main Menu, then select:

   2. Switch Configuration …
   4. Spanning Tree Operation

   You will then see the Spanning Tree screen with STP (802.1D) selected in the Protocol Version field (figure 6-17).
Spanning-Tree Operation
802.1D Spanning-Tree Protocol (STP)

In this example, ports 2 and 3 have already been configured as a port trunk (Trk1), which appears at the end of the port listing.

All ports (and the trunk) are in their default STP configuration.

Note: In the actual menu screen, you must scroll the cursor down the port list to view the trunk configuration (ports A2 and A3).

Figure 6-17. The Spanning Tree Operation Screen

4. On the ports and/or trunks you want to use for redundant fast uplink connections, change the mode to Uplink. In this example, port A1 and Trk1 (using ports A2 and A3) provide the redundant uplinks for STP:
   a. Press [E] (for Edit), then enable STP on the switch by using the Space bar to select Yes in the Spanning Tree Enabled field.
   b. Use [Tab] to move to the Mode field for port A1.
   c. Use the Space bar to select Uplink as the mode for port A1.
   d. Use [↓] to move to the Mode field for Trk1.
   e. Use the Space bar to select Uplink as the Mode for Trk1.
   f. Press [Enter] to return the cursor to the Actions line.
Spanning-Tree Operation
802.1D Spanning-Tree Protocol (STP)

--- CONSOLE - MANAGER MODE ---

Switch Configuration - Spanning Tree Operation

- Protocol Version: STP
  - STP Enabled [No]: No
  - Switch Priority [32768]: 32768
  - Hello Time [2]: 2
  - Max Age [20]: 20
  - Forward Delay [15]: 15

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Cost</th>
<th>Priority</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>10/100TX</td>
<td>100</td>
<td>128</td>
<td>Uplink</td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
<td>100</td>
<td>128</td>
<td>Norm</td>
</tr>
<tr>
<td>A5</td>
<td>10/100TX</td>
<td>100</td>
<td>128</td>
<td>Norm</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A24</td>
<td>10/100TX</td>
<td>100</td>
<td>128</td>
<td>Norm</td>
</tr>
<tr>
<td>Trk1</td>
<td></td>
<td>100</td>
<td>64</td>
<td>Uplink</td>
</tr>
</tbody>
</table>

Actions: Cancel Edit Save Help

---

Port A1 and Trk1 are now configured for fast-uplink STP.

---

Figure 6-18. Example of STP Enabled with Two Redundant Links Configured for Fast-Uplink STP

5. Press [S] (for Save) to save the configuration changes to flash (non-volatile) memory.

To View Fast-Uplink STP Status. Continuing from figures 6-17 and 6-18 in the preceding procedure, this task uses the same screen that you would use to view STP status for other operating modes.

1. From the Main Menu, select:
   - 1. Status and Counters ...
   - 7. Spanning Tree Information
Spanning-Tree Operation
802.1D Spanning-Tree Protocol (STP)

---

**Indicates which uplink is the active path to the STP root device.**

**Note:** A switch using fast-uplink STP must never be the STP root device.

---

Figure 6-19. Example of STP Status with Trk1 (Trunk 1) as the Path to the STP Root Device

2. Press [S] (for **Show ports**) to display the status of individual ports.

---

Figure 6-20. Example of STP Port Status with Two Redundant STP Links

---

6-38
In figure 6-20:

- Port A1 and Trk1 (trunk 1; formed from ports 2 and 3) are redundant fast-uplink STP links, with trunk 1 forwarding (the active link) and port A1 blocking (the backup link). (To view the configuration for port A1 and Trk1, see figure 6-18 on page 6-37.)
- If the link provided by trunk 1 fails (on both ports), then port A1 begins forwarding in fast-uplink STP mode.
- Ports A5, A6, and A24 are connected to end nodes and do not form redundant links.

CLI: Viewing and Configuring Fast-Uplink STP

Using the CLI to View Fast-Uplink STP. You can view fast-uplink STP using the same show commands that you would use for standard STP operation:

Syntax: show spanning-tree

Lists STP status.

Syntax: show spanning-tree config

Lists STP configuration for the switch and for individual ports.

For example, figures 6-21 and 6-22 illustrate a possible topology, STP status listing, and STP configuration for a Series 5300XL switch with:

- STP enabled and the switch operating as an Edge switch
- Port A1 and trunk 1 (Trk1) configured for fast-uplink STP operation
- Several other ports connected to PC or workstation end nodes

Figure 6-21. Example Topology for the Listing Shown in Figure 6-22
### HPswitch (config) # show spanning-tree

**Status and Counters - Spanning Tree Information**

- **STP Enabled**: Yes
- **Switch Priority**: 32768
- **Hello Time**: 2
- **Max Age**: 20
- **Forward Delay**: 15

- **Topology Change Count**: 25
- **Time Since Last Change**: 13 mins

- **Root MAC Address**: 0001e7-a09900
- **Root Path Cost**: 20
- **Root Port**: Trk1
- **Root Priority**: 16766

<table>
<thead>
<tr>
<th>Port</th>
<th>Type</th>
<th>Cost</th>
<th>Priority</th>
<th>State</th>
<th>Designated Bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Blocking</td>
<td>0030c1-e9c600</td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>A5</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Forwarding</td>
<td>0030c1-7fec40</td>
</tr>
<tr>
<td>A6</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Forwarding</td>
<td>0030c1-e9c600</td>
</tr>
<tr>
<td>A7</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Forwarding</td>
<td>0030c1-e9c622</td>
</tr>
<tr>
<td>A8</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>A9</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Forwarding</td>
<td>00a0c9-e234c3</td>
</tr>
<tr>
<td>A10</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Forwarding</td>
<td>0030c1-449bc0</td>
</tr>
<tr>
<td>A11</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>A12</td>
<td>10/100TX</td>
<td>10</td>
<td>128</td>
<td>Disabled</td>
<td></td>
</tr>
<tr>
<td>Trk1</td>
<td></td>
<td>10</td>
<td>64</td>
<td>Forwarding</td>
<td>0030c1-e9c800</td>
</tr>
</tbody>
</table>

**Figure 6-22. Example of a Show Spanning-Tree Listing for the Topology Shown in Figure 6-21**
Spanning-Tree Operation

802.1D Spanning-Tree Protocol (STP)

Figure 6-23. Example of a Configuration Supporting the STP Topology Shown in Figure 6-21

Using the CLI To Configure Fast-Uplink STP. This example uses the CLI to configure the switch for the fast-uplink operation shown in figures 6-21, 6-22, and 6-23. (The example assumes that ports A2 and A3 are already configured as members of the port trunk—Trk1, and all other STP parameters are left in their default state.)

Note that the default STP Protocol Version is RSTP (Rapid STP, or 802.1w). Thus, if the switch is set to the STP default, you must change it to the STP (802.1D) Protocol Version before you can configure Fast-Uplink. For example:

HPswitch(config)# show spanning-tree config
Spanning Tree Operation
  Spanning Tree Enabled: Yes
  STP Priority: 32768
  Max Age: 20
  Hello Time: 2
  Forward Delay: 15

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Cost</th>
<th>Pri Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>10/100TX</td>
<td>10 128 Uplink</td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>A5</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>A6</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>A7</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>A8</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>A9</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>A10</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>A11</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>A12</td>
<td>10/100TX</td>
<td>10 128 Norm</td>
</tr>
<tr>
<td>Trk1 Trunk</td>
<td>10 64 Uplink</td>
<td></td>
</tr>
</tbody>
</table>
Spanning-Tree Operation
802.1D Spanning-Tree Protocol (STP)

Syntax: spanning-tree <port/trunk-list> mode uplink

Enables STP on the switch and configures fast-uplink STP on the designated interfaces (port or trunk).

For example:

HPswitch(config)# spanning-tree e A1,trk1 mode uplink

Operating Notes

Effect of Reboots on Fast-Uplink STP Operation. When configured, fast-uplink STP operates on the designated ports in a running switch. However, if the switch experiences a reboot, the fast-uplink ports (Mode = Uplink) use the longer forwarding delay used by ports on standard 802.1D STP (non fast-uplink). This prevents temporary loops that could otherwise result while the switch is determining the STP status for all ports. That is, on ports configured for fast-uplink STP, the first STP state transition after a reboot takes the same amount of time as for redundant ports that are not configured for fast-uplink STP.

Using Fast Uplink with Port Trunks. To use a port trunk for fast-uplink STP, configure it in the same way that you would an individual port for the same purpose. A port trunk configured for fast uplink operates in the same way as an individual, non-trunked port operates; that is, as a logical port.
When you add a port to a trunk, the port takes on the STP mode configured for the trunk, regardless of which STP mode was configured on the port before it was added to the trunk. Thus, all ports belonging to a trunk configured with Uplink in the STP Mode field will operate in the fast-uplink mode. (If you remove a port from a trunk, the port reverts to the STP Mode setting it had before you added the port to the trunk.

To use fast uplink over a trunk, you must:

1. Create the trunk.
2. Configure the trunk for fast uplink in the same way that you would configure an individual port for fast uplink.

When you first create a port trunk, its STP Mode setting will be Norm, regardless of whether one or more ports in the trunk are set to fast uplink (Mode = Uplink). You must still specifically configure the trunk Mode setting to Uplink. Similarly, if you eliminate a trunk, the Mode setting on the individual ports in the trunk will return to their previous settings.


Web: Enabling or Disabling STP

In the web browser interface you can enable or disable STP on the switch. To configure other STP features, telnet to the switch console and use the CLI.

To enable or disable STP on the switch:

1. Click on the Configuration tab
2. Click on [Device Features].
3. Enable or disable STP.
4. Click on [Apply Changes] to implement the configuration change.

For web-based help on how to use the web browser interface screen, click on the [?] button provided on the web browser screen.
802.1s Multiple Spanning Tree Protocol (MSTP)

The 802.1D and 802.1w spanning tree protocols operate without regard to a network’s VLAN configuration, and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology. The 802.1s Multiple Spanning Tree protocol (MSTP) uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

While the per-VLAN spanning tree approach adopted by some vendors overcomes the network utilization problems inherent in using STP or RSTP, using a per-VLAN technology with multiple VLANs can overload the switch’s CPU. MSTP on the Switch 5300XL Series devices complies with the IEEE 802.1s standard, and extends STP and RSTP functionality to map multiple independent spanning tree instances onto a physical topology. With MSTP, each spanning tree instance can include one or more VLANs and applies a separate, per-instance forwarding topology. Thus, where a port belongs to multiple VLANs, it may be dynamically blocked in one spanning tree instance, but forwarding in another instance. This achieves load-balancing across the network while keeping the switch’s CPU load at a moderate level (by aggregating multiple VLANs in a single spanning tree instance). Like RSTP, MSTP provides fault tolerance through rapid, automatic reconfiguration if there is a failure in a network’s physical topology.

Caution

Spanning tree interprets a switch mesh as a single link. Because the switch automatically gives faster links a higher priority, the default MSTP parameter settings are usually adequate for spanning tree operation. Also, because incorrect MSTP settings can adversely affect network performance, you should not change the MSTP settings from their default values unless you have a strong understanding of how spanning tree operates.

In a mesh environment, the default MSTP timer settings (Hello Time and Forward Delay) are usually adequate for MSTP operation. Because a packet crossing a mesh may traverse several links within the mesh, using smaller-than-default settings for the MSTP Hello Time and Forward Delay timers can cause unnecessary topology changes and end-node connectivity problems.

For MSTP information beyond what is provided in this manual, refer to the IEEE 802.1s standard.
MSTP Structure

MSTP maps active, separate paths through separate spanning tree instances and between MST regions. Each MST region comprises one or more MSTP switches. Note that MSTP recognizes an STP or RSTP LAN as a distinct spanning-tree region.

![Diagram of MSTP Network](image)

**Figure 6-25. Example of MSTP Network with Legacy STP and RSTP Devices Connected**

**Common and Internal Spanning Tree (CIST):** The CIST identifies the regions in a network and administers the CIST root bridge for the network, the root bridge for each region, and the root bridge for each spanning-tree instance in each region.

**Common Spanning Tree (CST):** The CST administers the connectivity among the MST regions, STP LANs, and RSTP LANs in a bridged network.
**MST Region:** An MST region comprises the VLANs configured on physically connected MSTP switches. All switches in a given region must be configured with the same VLANs and Multiple Spanning Tree Instances (MSTIs).

**Internal Spanning Tree (IST):** The IST administers the topology within a given MST region. When you configure a switch for MSTP operation, the switch automatically includes all of the static VLANs configured on the switch in a single, active spanning tree topology (instance) within the IST. This is termed the “IST instance”. Any VLANs you subsequently configure on the switch are added to this IST instance. To create separate forwarding paths within a region, group specific VLANs into different Multiple Spanning Tree Instances (MSTIs). (Refer to “Multiple Spanning Tree Instance”, below.)

**Types of Multiple Spanning Tree Instances:** A multiple spanning tree network comprises separate spanning-tree instances existing in an MST region. (There can be multiple regions in a network.) Each instance defines a single forwarding topology for an exclusive set of VLANs. By contrast, an STP or RSTP network has only one spanning tree instance for the entire network, and includes all VLANs in the network. (An STP or RSTP network operates as a single-instance network.) A region can include two types of STP instances:

- **Internal Spanning-Tree Instance (IST Instance):** This is the default spanning tree instance in any MST region. It provides the root switch for the region and comprises all VLANs configured on the switches in the region that are not specifically assigned to Multiple Spanning Tree Instances (MSTIs, described below). All VLANs in the IST instance of a region are part of the same, single spanning tree topology, which allows only one forwarding path between any two nodes belonging to any of the VLANs included in the IST instance. All switches in the region must belong to the set of VLANs that comprise the IST instance. Note that the switch automatically places dynamic VLANs (resulting from GVRP operation) in the IST instance. Dynamic VLANs cannot exist in an MSTI (described below).

- **MSTI (Multiple Spanning Tree Instance):** This type of configurable spanning tree instance comprises all static VLANs you specifically assign to it, and must include at least one VLAN. The VLAN(s) you assign to an MSTI must initially exist in the IST instance of the same MST region. When you assign a static VLAN to an MSTI, the switch removes the VLAN from the IST instance. (Thus, you can assign a VLAN to only one MSTI in a given region.) All VLANs in an MSTI operate as part of the same single spanning tree topology. (The switch does not allow dynamic VLANs in an MSTI.)
Caution

When you enable MSTP on the switch, the default MSTP spanning tree configuration settings comply with the values recommended in the IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) standard. Note that inappropriate changes to these settings can result in severely degraded network performance. For this reason, HP strongly recommends that changing these default settings be reserved only for experienced network administrators who have a strong understanding of the IEEE 802.1D/w/s standards and operation.

How MSTP Operates

In the factory default configuration, spanning tree operation is off. Also, the switch retains its currently configured spanning tree parameter settings when disabled. Thus, if you disable spanning tree, then later re-enable it, the parameter settings will be the same as before spanning tree was disabled. The switch also includes a “Pending” feature that enables you to exchange MSTP configurations with a single command. (Refer to “Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another” on page 6-69.)

Note

The switch automatically senses port identity and type, and automatically defines spanning-tree parameters for each type, as well as parameters that apply across the switch. Although these parameters can be adjusted, HP strongly recommends leaving these settings in their default configurations unless the proposed changes have been supplied by an experienced network administrator who has a strong understanding of the IEEE 802.1D/w/s standards and operation.

MST Regions

All MSTP switches in a given region must be configured with the same VLANs. Also, each MSTP switch within the same region must have the same VLAN-to-instance assignments. (A VLAN can belong to only one instance within any region.) Within a region:

- All of the VLANs belonging to a given instance compose a single, active spanning-tree topology for that instance.
- Each instance operates independently of other regions.

Between regions there is a single, active spanning-tree topology.
How Separate Instances Affect MSTP Operation. Assigning different groups of VLANs to different instances ensures that those VLAN groups use independent forwarding paths. For example, in figure 6-26 each instance has a different forwarding path.

Figure 6-26. Active Topologies Built by Three Independent MST Instances

While allowing only one active path through a given instance, MSTP retains any redundant physical paths in the instance to serve as backups (blocked) paths in case the existing active path fails. Thus, if an active path in an instance fails, MSTP automatically activates (unblocks) an available backup to serve as the new active path through the instance for as long as the original active path is down. Note also that a given port may simultaneously operate in different states (forwarding or blocking) for different spanning-tree instances within the same region. This depends on the VLAN memberships to which the port is assigned. For example, if a port belongs to VLAN 1 in the IST instance of a region and also belongs to VLAN 4 in MSTI “x” in the same region, the port may apply different states to traffic for these two different instances.
Within a region, traffic routed between VLANs in separate instances can take only one physical path. To ensure that traffic in all VLANs within a region can travel between regions, all of the boundary ports for each region should belong to all VLANs configured in the region. Otherwise, traffic from some areas within a region could be blocked from moving to other regions.

All MSTP switches (as well as STP and RSTP switches) in a network use BPDUs (Bridge Protocol Data Units) to exchange information from which to build multiple, active topologies in the individual instances within a region and between regions. From this information:

- The MSTP switches in each LAN segment determine a designated bridge and designated port or trunk for the segment.
- The MSTP switches belonging to a particular instance determine the root bridge and root port or trunk for the instance.
- For the IST instance within a region, the MSTP switches linking that region to other regions (or to STP or RSTP switches) determine the IST root bridge and IST root port or trunk for the region. (For any Multiple Spanning-Tree instance—MSTI—in a region, the regional root may be a different switch that is not necessarily connected to another region.)
- The MSTP switches block redundant links within each LAN segment, across all instances, and between regions, to prevent any traffic loops.

As a result, each individual instance (spanning tree) within a region determines its regional root bridge, designated bridges, and designated ports or trunks.

Regions, Legacy STP and RSTP Switches, and the Common Spanning Tree (CST)

The IST instance and any MST instances in a region exist only within that region. Where a link crosses a boundary between regions (or between a region and a legacy STP or RSTP switch), traffic is forwarded or blocked as determined by the Common Spanning Tree (CST). The CST ensures that there is only one active path between any two regions, or between a region and a switch running STP and RSTP. (Refer to figure 6-25 on page 6-45.)

MSTP Operation with 802.1Q VLANs

As indicated in the preceding sections, within a given MST instance, a single spanning tree is configured for all VLANs included in that instance. This means that if redundant physical links exist in separate VLANs within the same instance, MSTP blocks all but one of those links. However, you can prevent the bandwidth loss caused by blocked redundant links for different VLANs in
an instance by using a port trunk. The following example shows how you can use a port trunk with 802.1Q (tagged) VLANs and MSTP without unnecessarily blocking any links or losing any bandwidth.

**Problem:**
An MST instance with two separate (non-trunked) links blocks a VLAN link.

**Solution:**
Configure one trunked link for the two VLAN memberships.

Nodes 1 and 2 cannot communicate because MSTP is blocking the link.

Nodes 1 and 2 can communicate because the MST instance sees the trunk as a single link and 802.1Q (tagged) VLANs enable the use of one (trunked) link for both VLANs.

---

**Note**
All switches in a region should be configured with the VLANs used in that region, and all ports linking MSTP switches together should be members of all VLANs in the region. Otherwise, the path to the root for a given VLAN will be broken if MSTP selects a spanning tree through a link that does not include that VLAN.

**Terminology**

**Bridge:** See “MSTP Bridge”.

**Common and Internal Spanning Tree (CIST):** Comprises all LANs, STP, and RSTP bridges and MSTP regions in a network. The CIST automatically determines the MST regions in a network and defines the root bridge (switch)
and designated port for each region. The CIST includes the Common Spanning Tree (CST), the Internal Spanning Tree (IST) within each region, and any multiple spanning-tree instances (MSTIs) in a region.

**Common Spanning Tree (CST):** Refers to the single forwarding path the switch calculates for STP (802.1D) and RSTP (802.1w) topologies, and for inter-regional paths in MSTP (802.1s) topologies. Note that all three types of spanning tree can interoperate in the same network. Also, the MSTP switch interprets a device running 802.1D STP or 802.1w RSTP as a separate region. (Refer to figure 6-25 on page 6-45.)

**Internal Spanning Tree (IST):** Comprises all VLANs within a region that are not assigned to a multiple spanning-tree instance configured within the region. All MST switches in a region should belong to the IST. In a given region “X”, the IST root switch is the regional root switch and provides information on region “X” to other regions.

**MSTP (Multiple Spanning Tree Protocol):** A network supporting MSTP allows multiple spanning tree instances within configured regions, and a single spanning tree among regions, STP bridges, and RSTP bridges.

**MSTP BPDU (MSTP Bridge Protocol Data Unit):** These BPDUs carry region-specific information, such as the region identifier (region name and revision number). If a switch receives an MSTP BPDU with a region identifier that differs from its own, then the port on which that BPDU was received is on the boundary of the region in which the switch resides.

**MSTP Bridge:** In this manual, an MSTP bridge is an HP ProCurve Switch 5300XL Series device (or another 802.1s-compatible device) configured for MSTP operation.

**MST Region:** An MST region forms a multiple spanning tree domain and is a component of a single spanning-tree domain within a network. For switches internal to the MST region:
- All switches have identical MST configuration identifiers (region name and revision number).
- All switches have identical VLAN assignments to the region’s IST and (optional) MST instances.
- One switch functions as the designated bridge (IST root) for the region.
- No switch has a point-to-point connection to a bridging device that cannot process RSTP BPDUs.
Operating Rules

- All switches in a region must be configured with the same set of VLANs, as well as the same MST configuration name and MST configuration number.
- Within a region, a VLAN can be allocated to either a single MSTI or to the region’s IST instance.
- All switches in a region must have the same VID-to-MST instance and VID-to-IST instance assignments.
- There is one root MST switch per configured MST instance.
- Within any region, the root switch for the IST instance is also the root switch for the region. Because boundary ports provide the VLAN connectivity between regions, all boundary ports on a region’s root switch should be configured as members of all static VLANs defined in the region.
- There is one root switch for the Common and Internal Spanning Tree (CIST). Note that the per-port hello-time parameter assignments on the CIST root switch propagate to the ports on downstream switches in the network and override the hello-time configured on the downstream switch ports.
- Where multiple MST regions exist in a network, there is only one active, physical communication path between any two regions, or between an MST region and an STP or RSTP switch. MSTP blocks any other physical paths as long as the currently active path remains in service.
- Within a network, an MST region appears as a virtual RSTP bridge to other spanning tree entities (other MST regions, and any switches running 802.1D or 802.1w spanning-tree protocols).
- Within an MSTI, there is one spanning tree (one physical, communication path) between any two nodes. That is, within an MSTI, there is one instance of spanning tree, regardless of how many VLANs belong to the MSTI. Within an IST instance, there is also one spanning tree across all VLANs belonging to the IST instance.
- An MSTI comprises a unique set of VLANs and forms a single spanning-tree instance within the region to which it belongs.
- Communication between MST regions uses a single spanning tree.
- If a port on a switch configured for MSTP receives a legacy (STP/802.1D or RSTP/802.1w) BPDU, it automatically operates as a legacy port. In this case, the MSTP switch interoperates with the connected STP or RSTP switch as a separate MST region.
- Within an MST region, there is one logical forwarding topology per instance, and each instance comprises a unique set of VLANs. Where multiple paths exist between a pair of nodes using VLANs belonging to
the same instance, all but one of those paths will be blocked for that instance. However, if there are different paths in different instances, all such paths are available for traffic. Separate forwarding paths exist through separate spanning tree instances.

- A port can have different states (forwarding or blocking) for different instances (which represent different forwarding paths).
- MSTP interprets a switch mesh as a single link.
- A dynamic VLAN learned by GVRP will always be placed in the IST instance and cannot be moved to any configured MST instance.

**Transitioning from STP or RSTP to MSTP**

IEEE 802.1s MSTP includes RSTP functionality and is designed to be compatible with both IEEE 802.1D and 802.1w spanning-tree protocols. Even if all the other devices in your network are using STP, you can enable MSTP on your 5300XL switches. Also, using the default configuration values, your 5300XL switches will interoperate effectively with STP and RSTP devices. MSTP automatically detects when the switch ports are connected to non-MSTP devices in the spanning tree and communicates with those devices using 802.1D or 802.1w STP BPDU packets, as appropriate.

Because MSTP is so efficient at establishing the network path, HP highly recommends that you update all of your 5300XL switches to support MSTP. (For switches that do not support 802.1s, HP recommends that you update to RSTP to benefit from the convergence times of less than one second under optimal circumstances.) To make the best use of MSTP and achieve the fastest possible convergence times, there are some changes that you should make to the MSTP default configuration.

**Note**

Under some circumstances, it is possible for the rapid state transitions employed by MSTP and RSTP to result in an increase in the rates of frame duplication and misordering in the switched LAN. In order to allow MSTP and RSTP switches to support applications and protocols that may be sensitive to frame duplication and misordering, setting the Force Protocol Version parameter to **STP-compatible** allows MSTP and RSTP to operate with the rapid transitions disabled. The value of this parameter applies to all ports on the switch. See information on **force version** on page 6-14.

As indicated above, one of the benefits of MSTP and RSTP is the implementation of a larger range of port path costs, which accommodates higher network speeds. New default values have also been implemented for the path costs associated with the different network speeds. This can create some
incompatibility between devices running the older 802.1D STP and your switch running MSTP or RSTP. Please see the “Note on Path Cost” on page 6-17 for more information on adjusting to this incompatibility.

Tips for Planning an MSTP Application

- Ensure that the VLAN configuration in your network supports all of the forwarding paths necessary for the desired connectivity. All ports connecting one switch to another within a region and one switch to another between regions should be configured as members of all VLANs configured in the region.

- All ports or trunks connecting one switch to another within a region should be configured as members of all VLANs in the region. Otherwise, some VLANs could be blocked from access to the spanning-tree root for an instance or for the region.

- Plan individual regions based on VLAN groupings. That is, plan on all MSTP switches in a given region supporting the same set of VLANs. Within each region, determine the VLAN membership for each spanning-tree instance. (Each instance represents a single forwarding path for all VLANs in that instance.)

- There is one logical spanning-tree path through the following:
  - Any inter-regional links
  - Any IST or MST instance within a region
  - Any legacy (802.1D or 802.1w) switch or group of switches. (Where multiple paths exist between an MST region and a legacy switch, expect the CST to block all but one such path.)

- Determine the root bridge and root port for each instance.

- Determine the designated bridge and designated port for each LAN segment.

- Determine which VLANs to assign to each instance, and use port trunks with 802.1Q VLAN tagging where separate links for separate VLANs would result in a blocked link preventing communication between nodes on the same VLAN. (Refer to “MSTP Operation with 802.1Q VLANs” on page 6-49.)

- Identify the edge ports connected to end nodes and enable the edge-port setting for these ports. Leave the edge-port setting disabled for ports connected to another switch, a bridge, or a hub.
Note on MSTP Rapid State Transitions

Under some circumstances the rapid state transitions employed by MSTP (and RSTP) can increase the rates of frame duplication and misordering in the switched LAN. To allow MSTP switches to support applications and protocols that may be sensitive to frame duplication and misordering, setting the Force Protocol Version (force-version) parameter to stp-compatible allows MSTP to operate with rapid transitions disabled. The value of this parameter applies to all ports on the switch. See the information on force-version on page 6-60.

Steps for Configuring MSTP

This section outlines the general steps for configuring MSTP operation in your network, and assumes you have already planned and configured the VLANs you want MSTP to use. The actual MSTP parameter descriptions are in the following sections.

Note

The switch supports MSTP configuration through the CLI. After you specify MSTP and reboot the switch as described above, the switch removes the Spanning Tree option from the Menu interface. If you later reconfigure the switch to use STP or RSTP, the switch returns the Spanning Tree option to the Menu interface.

This section assumes that you have already

1. Configured the MSTP operation mode. This specifies MSTP as the spanning tree operating mode. Changing the current MSTP operation mode requires you to save the change and reboot to activate the selection.

   spanning-tree protocol-version < stp | rstp | mstp >

2. Configure MSTP global parameters. This step involves configuring the following:
   - Required parameters for MST region identity:
     Region Name: spanning-tree config-name
     Region Revision Number: spanning-tree config revision
   - Optional MSTP parameter changes for region settings:

     HP recommends that you leave these parameters at their default settings for most networks. Refer to the “Caution” on page 6-47.
     - The maximum number of hops before the MSTP BPDU is discarded (default: 20)
       spanning-tree max-hops
Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

- Force-Version operation
  `spanning-tree force-version`

- Forward Delay
  `spanning-tree forward-delay`

- Hello Time (used if the switch operates as the root device.)
  `spanning-tree hello-time`

- Maximum age to allow for STP packets before discarding
  `spanning-tree max-age`

- Device spanning-tree priority. Specifies the priority value used along with the switch MAC address to determine which device is root. The lower a priority value, the higher the priority.
  `spanning-tree priority`

3. Configure MST instances.
   - Configure one instance for each VLAN group that you want to operate as an active topology within the region to which the switch belongs. When you create the instance, you must include a minimum of one VID. You can add more VIDs later if desired.
     `spanning-tree instance < 1 - 16 > vlan < vid >`

     To move a VLAN from one instance to another, first use `no spanning-tree instance < n > vlan < vid >` to unmap the VLAN from the current instance, then add the VLAN to the other instance. (While the VLAN is unmapped from an MSTI, it is associated with the region’s IST instance.)
   - Configure the priority for each instance.
     `spanning-tree instance`

4. Configure MST instance port parameters. Enable `edge-port` for ports connected to end nodes (page 6-61), but leave it disabled (the default) for connections to another switch, a bridge, or a hub. Set the path cost value for the port(s) used by a specific MST instance. Leaving this setting at the default auto allows the switch to calculate the path-cost from the link speed.
   `spanning-tree instance < 1 - 16 | ist > [ E ] port-list < port-list >`

5. Enable spanning-tree operation on the switch.
   `spanning-tree`
Configuring MSTP Operation Mode and Global Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree protocol-version mstp</td>
<td>6-58</td>
</tr>
<tr>
<td>spanning-tree config-name &lt; ascii-string &gt;</td>
<td>6-58</td>
</tr>
<tr>
<td>spanning-tree config-revision &lt; revision-number &gt;</td>
<td>6-59</td>
</tr>
<tr>
<td>spanning-tree max-hops &lt; hop-count &gt;</td>
<td>6-59</td>
</tr>
<tr>
<td>spanning-tree force-version</td>
<td>6-60</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The commands in this section apply on the switch level, and do not affect individual port configurations.
Spanning-Tree Operation

802.1s Multiple Spanning Tree Protocol (MSTP)

Syntax: spanning-tree-protocol-version mstp

Changes the current spanning-tree protocol on the switch to 802.1s Multiple Spanning Tree. Must be followed by write mem and reboot to activate the change. After rebooting, the switch is ready to operate as an MSTP bridge. Note that this command does not enable spanning-tree operation. To activate the configured spanning-tree operation on the switch, execute spanning-tree.

Note: When you activate spanning-tree operation or change the spanning-tree configuration while spanning tree is enabled, the switch must recalculate the network paths it uses. To minimize traffic delays while this convergence occurs, HP recommends that you not activate spanning tree operation until you have finished configuring all devices in your network. Refer to “Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another” on page 6-69.

The following commands are available only when the switch is configured for MSTP protocol operation.

Syntax: [no] spanning-tree config-name < ascii-string >

This command resets the the configuration name of the MST region in which the switch resides. This name can include up to 32 nonblank characters and is case-sensitive. On all switches within a given MST region, the configuration names must be identical. Thus, if you want more than one MSTP switch in the same MST region, you must configure the identical region name on all such switches. If you retain the default configuration name on a switch, it cannot exist in the same MST region with another switch. (Default Name: A text string using the hexadecimal representation of the switch’s MAC address)

The no form of the command overwrites the currently configured name with the default name.

Note: This option is available only when the switch is configured for MSTP operation. Also, there is no defined limit on the number of regions you can configure.
Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

**Syntax:** spanning-tree config-revision < revision-number >

This command configures the revision number you designate for the MST region in which you want the switch to reside. This setting must be the same for all switches residing in the same region. Use this setting to differentiate between region configurations in situations such as the following:

- Changing configuration settings within a region where you want to track the configuration versions you use
- Creating a new region from a subset of switches in a current region and want to maintain the same region name.
- Using the pending option to maintain two different configuration options for the same physical region.

Note that this setting must be the same for all MSTP switches in the same MST region. (Range: 0 - 65535; Default: 0)

**Note:** This option is available only when the switch is configured for MSTP operation.

**Syntax:** spanning-tree max-hops < hop-count >

This command resets the number of hops allowed for BPDUs in an MST region. When an MSTP switch receives a BPDU, it decrements the hop-count setting the BPDU carries. If the hop-count reaches zero, the receiving switch drops the BPDU. Note that the switch does not change the message-age and maximum-age data carried in the BPDU as it moves through the MST region and is propagated to other regions. (Range: 1 - 40; Default: 20)
**Spanning-Tree Operation**

**802.1s Multiple Spanning Tree Protocol (MSTP)**

**Syntax:** spanning-tree force-version < stp-compatible | rstp-operation | mstp-operation >

Sets the spanning-tree compatibility mode. When the switch is configured with MSTP mode, this command forces the switch to emulate behavior of earlier versions of spanning tree protocol or return to MSTP behavior. The command is useful in test or debug applications, and removes the need to reconfigure the switch for temporary changes in spanning-tree operation.

**stp-compatible:** The switch applies 802.1D STP operation on all ports.

**rstp-operation:** The switch applies 802.1w operation on all ports except those ports where it detects a system using 802.1D Spanning Tree.

**mstp-operation:** The switch applies 802.1s MSTP operation on all ports where compatibility with 802.1D or 802.1w spanning tree protocols is not required.

This command is available when the protocol version is set to mstp (see 'protocol-version' later).

Note that even when mstp-operation is selected, if the switch detects an 802.1D BPDU or an 802.1w BPDU on a port, it communicates with the device linked to that port using STP or RSTP BPDU packets. Also, if errors are encountered as described in the “Note on MSTP Rapid State Transitions” on page 6-55, setting force-version to stp-compatible forces the MSTP switch to communicate out all ports using operations that are compatible with IEEE 802.1D STP.

**Syntax:** spanning-tree hello-time < 1..10 >

If MSTP is running and the switch is operating as the CIST root for your network, this command specifies the time in seconds between transmissions of BPDUs for all ports on the switch configured with Use Global (the default). This parameter applies in MSTP, RSTP and STP modes. During MSTP operation, you can override this global setting on a per-port basis with this command: spanning-tree < port-list > hello-time < 1..10 > (page 6-61). (Default: 2.)
Configuring Basic Port Connectivity Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree &lt; port-list &gt;</td>
<td></td>
</tr>
<tr>
<td>edge-port</td>
<td>below</td>
</tr>
<tr>
<td>spanning-tree mcheck</td>
<td>below</td>
</tr>
<tr>
<td>hello-time &lt; global</td>
<td>1..10 &gt;</td>
</tr>
<tr>
<td>spanning-tree path-cost &lt; auto l 200000000 &gt;</td>
<td>6-64</td>
</tr>
<tr>
<td>spanning-tree point-to-point-mac &lt; force-true</td>
<td>force-false</td>
</tr>
<tr>
<td>spanning-tree priority</td>
<td>6-65</td>
</tr>
</tbody>
</table>

The basic port connectivity parameters affect spanning-tree links at the global level. In most cases, HP recommends that you use the default settings for these parameters and apply changes on a per-port basis only where a nondefault setting is clearly indicated by the circumstances of individual links.

**Syntax:** [no] spanning-tree < port-list > < edge-port | mcheck >

  [ edge-port ]

  *Enable edge-port on ports connected to end nodes. During spanning tree establishment, ports with edge-port enabled transition immediately to the forwarding state. Disable this feature on any switch port that is connected to another switch, bridge, or hub. (Default: No - disabled)*

  *The no spanning-tree < port-list > edge-port command disables edge-port operation on the specified ports.*

  [ mcheck ]

  *Forces a port to send RSTP BPDUs for 3 seconds. This allows for another switch connected to the port and running RSTP to establish its connection quickly and for identifying switches running 802.1D STP. If the whole-switch force-version parameter is set to stp-compatible, the switch ignores the mcheck setting and sends 802.1D STP BPDUs out all ports. Disable this feature on all ports that are known to be connected to devices that are running 802.1D STP. (Default: Yes - enabled)*

  *The no spanning-tree < port-list > mcheck command disables mcheck.*
**Syntax:** spanning-tree <port-list> <hello-time | path-cost | point-to-point-mac | priority >

[ hello-time < global | 1 - 10 >

When the switch is the CIST root, this parameter specifies the interval (in seconds) between periodic BPDU transmissions by the designated ports. This interval also applies to all ports in all switches downstream from each port in the <port-list>. A setting of global indicates that the ports in <port-list> on the CIST root are using the value set by the global spanning-tree hello-time value (page 6-60). When a given switch “X” is not the CIST root, the per-port hello-time for all active ports on switch “X” is propagated from the CIST root, and is the same as the hello-time in use on the CIST root port in the currently active path from switch “X” to the CIST root. (That is, when switch “X” is not the CIST root, then the upstream CIST root’s port hello-time setting overrides the hello-time setting configured on switch “X”. (Default Per-Port setting: Use Global. Default Global Hello-Time: 2.)

[ path-cost < auto | 1..200000000 > ]

Assigns an individual port cost that the switch uses to determine which ports are forwarding ports in a given spanning tree. In the default configuration (auto) the switch determines a port’s path cost by the port’s type:

- 10 Mbps: 2000000
- 100 Mbps: 200000
- 1 Gbps: 20000

Refer to “Note on Path Cost” on page 6-17 for information on compatibility with devices running 802.1D STP for the path cost values (Default: Auto.).

defined-to-point-mac < force-true | force-false | auto >

This parameter informs the switch of the type of device to which a specific port connects.

**Force-True (default):** Indicates a point-to-point link to a device such as a switch, bridge, or end-node.

**Force-False:** Indicates a connection to a hub (which is a shared LAN segment).

**Auto:** Causes the switch to set Force-False on the port if it is not running at full duplex. (Connections to hubs are half-duplex.)
Configuring MST Instance Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree instance &lt; 1..16 &gt; vlan &lt; vid&gt; [ vid..vid ]</td>
<td>6-61</td>
</tr>
<tr>
<td>no spanning-tree instance &lt; 1..16 &gt;</td>
<td></td>
</tr>
<tr>
<td>spanning-tree instance &lt; 1..16 &gt; priority &lt; 0..15 &gt;</td>
<td>6-63</td>
</tr>
<tr>
<td>spanning-tree priority &lt; 0..15 &gt;</td>
<td>6-64</td>
</tr>
</tbody>
</table>

**Syntax:** spanning-tree instance < 1..16 > vlan < vid [ vid..vid ] >
no spanning-tree instance < 1..16 >

Configuring MSTP on the switch automatically configures the IST instance and places all statically configured VLANs on the switch into the IST instance. This command creates a new MST instance (MSTI) and moves the VLANs you specify from the IST to the MSTI. At least one VLAN must be mapped to a MSTI when you create it. (A VLAN cannot be mapped to more than one instance at a time.) You can create up to 16 MSTIs in a region. Use the no form of the command to remove a VLAN from an MSTI. (Removing a VLAN from an MSTI returns the VLAN to the IST instance, where it can either remain or be re-assigned to another MSTI configured in the region.)

The no form of the command deletes the specified MSTI and returns all VLAN assignments to the region’s IST instance.
Syntax: spanning-tree instance <1..16> priority <0..15>

This command sets the switch (bridge) priority for the designated instance. This priority is compared with the priorities of other switches in the same instance to determine the root switch for the instance. The lower the priority value, the higher the priority. (If there is only one switch in the instance, then that switch is the root switch for the instance.) The root bridge in a given instance provides the path to connected instances in other regions that share one or more of the same VLAN(s). (Traffic in VLANs assigned to a numbered STP instance in a given region moves to other regions through the root switch for that instance.)

The priority range for an MSTP switch is 0-61440. However, this command specifies the instance priority as a multiplier (0 - 15) of 4096. That is, when you specify an instance priority value of 0 - 15, the actual priority assigned to the switch for the specified MST instance is:

\[(\text{instance-priority-value}) \times 4096\]

For example, if you configure “5” as the priority for MST Instance 1 on a given MSTP switch, then the Switch Priority setting is 20,480 for that instance in that switch.

Note: If multiple switches in the same MST instance have the same priority setting, then the switch with the lowest MAC address becomes the root switch for that instance.
**Syntax:** spanning-tree priority < 0 .. 15 >

This command sets the switch (bridge) priority for the designated region in which the switch resides. The switch compares this priority with the priorities of other switches in the same region to determine the root switch for the region. The lower the priority value, the higher the priority. (If there is only one switch in the region, then that switch is the root switch for the region.) The root bridge in a region provides the path to connected regions for the traffic in VLANs assigned to the region’s IST instance. (Traffic in VLANs assigned to a numbered STP instance in a given region moves to other regions through the root switch for that instance.)

The priority range for an MSTP switch is 0-61440. However, this command specifies the priority as a multiplier (0 - 15) of 4096. That is, when you specify a priority value of 0 - 15, the actual priority assigned to the switch is:

\[(\text{priority-value}) \times 4096\]

For example, if you configure “2” as the priority on a given MSTP switch, then the **Switch Priority** setting is 8,192.

**Note:** If multiple switches in the same MST region have the same priority setting, then the switch with the lowest MAC address becomes the root switch for that region.
Configuring MST Instance Per-Port Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree instance &lt; 1..16 &gt; &lt; port-list &gt; path-cost &lt; auto</td>
<td>6-66</td>
</tr>
<tr>
<td>spanning-tree instance &lt; 1..16 &gt; &lt; port-list &gt; priority &lt; priority-multiplier&gt;</td>
<td>6-67</td>
</tr>
<tr>
<td>spanning-tree &lt; port-list &gt; priority &lt; priority-multiplier &gt;</td>
<td>6-68</td>
</tr>
</tbody>
</table>

**Syntax:** spanning-tree instance < 1..16 > [e] < port-list > path-cost < auto | 1..200000000 >

*This command assigns an individual port cost for the specified MST instance. (For a given port, the path cost setting can be different for different MST instances to which the port may belong.) The switch uses the path cost to determine which ports are the forwarding ports in the instance; that is which links to use for the active topology of the instance and which ports to block. The settings are either auto or in a range from 1 to 200,000,000. With the auto setting, the switch calculates the path cost from the link speed:

- 10 Mbps — 2000000
- 100 Mbps — 200000
- 1 Gbps — 20000

(Default: Auto)
Syntax: spanning-tree instance < 1..16 > [e] < port-list > priority < priority-multiplier >

This command sets the priority for the specified port(s) in the specified MST instance. (For a given port, the priority setting can be different for different MST instances to which the port may belong.) The priority range for a port in a given MST instance is 0-255. However, this command specifies the priority as a multiplier (0 - 15) of 16. That is, when you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

\[(\text{priority-multiplier}) \times 16\]

For example, if you configure “2” as the priority multiplier on a given port in an MST instance, then the actual Priority setting is 32. Thus, after you specify the port priority multiplier in an instance, the switch displays the actual port priority (and not the multiplier) in the show spanning-tree instance < 1..16 > or show spanning-tree < port-list > instance < 1..16 > displays.

You can view the actual multiplier setting for ports in the specified instance by executing show running and looking for an entry in this format:

spanning-tree instance < 1..15 > < port-list > priority < priority-multiplier >

For example, configuring port A2 with a priority multiplier of “3” in instance 1, results in this line in the show running output:

spanning-tree instance 1 A2 priority 3
Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

Syntax: spanning-tree [e] < port-list > priority < priority-multiplier >

This command sets the priority for the specified port(s) for the IST (that is, Instance 0) of the region in which the switch resides. This priority is compared with the priorities of other ports in the IST to determine which port is the root port for the IST instance. The lower the priority value, the higher the priority. The IST root port (or trunk) in a region provides the path to connected regions for the traffic in VLANs assigned to the region’s IST instance.

The priority range for a port in a given MST instance is 0-240. However, this command specifies the priority as a multiplier (0 - 15) of 16. That is, when you specify a priority multiplier of 0 - 15, the actual priority assigned to the switch is:

\[(\text{priority-multiplier}) \times 16\]

For example, configuring “5” as the priority multiplier on a given port in the IST instance for a region creates an actual Priority setting of 80. Thus, after you specify the port priority multiplier for the IST instance, the switch displays the actual port priority (and not the multiplier) in the show spanning-tree instance ist or show spanning-tree < port-list > instance ist displays. You can view the actual multiplier setting for ports in the IST instance by executing show running and looking for an entry in this format:

spanning-tree < port-list > priority < priority-multiplier >

For example, configuring port A2 with a priority multiplier of “2” in the IST instance, results in this line in the show running output:

spanning-tree A2 priority 2
Enabling or Disabling Spanning Tree Operation

This command enables or disables spanning tree operation for any spanning tree protocol enabled on the switch. Before using this command to enable spanning tree, ensure that the version you want to use is active on the switch.

**Syntax:** [no] spanning-tree

Enabling spanning tree with MSTP configured implements MSTP for all physical ports on the switch, according to the VLAN groupings for the IST instance and any other configured instances. Disabling MSTP removes protection against redundant loops that can significantly slow or halt a network. This command simply turns spanning tree on or off. It does not change the existing spanning tree configuration.

Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning-tree pending &lt; apply</td>
<td>config-name</td>
</tr>
</tbody>
</table>

This operation exchanges the currently active MSTP configuration with the currently pending MSTP configuration. It enables you to implement a new MSTP configuration with minimal network disruption or to exchange MSTP configurations for testing or troubleshooting purposes.

When you configure or reconfigure MSTP, the switch re-calculates the corresponding network paths. This can have a ripple effect throughout your network as adjacent MSTP switches recalculate network paths to support the configuration changes invoked in a single switch. Although MSTP employs RSTP operation, the convergence time for implementing MSTP changes can be disruptive to your network. However, by using the spanning-tree pending feature, you can set up an MSTP on the switch and then invoke all instances of the new configuration at the same time, instead of one at a time.

**To Create a Pending MSTP Configuration.** This procedure creates a pending MSTP configuration and exchanges it with the active MSTP configuration.
1. Configure the VLANs you want included in any instances in the new region. When you create the pending region, all VLANs configured on the switch will be assigned to the pending IST instance unless assigned to other, pending MST instances.

2. Configure MSTP as the spanning-tree protocol, then execute `write mem` and reboot. (The pending option is available only with MSTP enabled.)

3. Configure the pending region name to assign to the switch.

4. Configure the pending `config-revision` number for the region name.

5. If you want an MST instance other than the IST instance, configure the instance number and assign the appropriate VLANs (VIDs). (The `pending` command creates the region's IST instance automatically.)

6. Repeat step 5 for each additional MST instance you want to configure.

7. Use the `show spanning-tree pending` command to review your pending configuration (page 6-77).

8. Use the `spanning-tree pending apply` command to exchange the currently active MSTP configuration with the pending MSTP configuration.

**Syntax:** spanning-tree pending < apply | config-name | config-revision | instance | reset >

- **apply**
  
  *Exchanges the currently active MSTP configuration with the pending MSTP configuration.*

- **config-name**
  
  *Specifies the pending MST region name. Must be the same for all MSTP switches in the region. (Default: The switch’s MAC address.)*

- **config-revision**
  
  *Specifies the pending MST region configuration revision number. Must be the same for all MSTP switches in the region. (Default: 0).*

- **instance < 1..16 > vlan [ < vid | vid-range > ]**
  
  *Creates the pending instance and assigns one or more VLANs to the instance.*

- **reset**
  
  *Copies the switch’s currently active MSTP configuration to the pending configuration. This is useful when you want to experiment with the current MSTP configuration while maintaining an unchanged version.*
9. To view the current pending MSTP configuration, use the `show spanning-tree pending` command (page 6-77).

Displaying MSTP Statistics and Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MSTP Statistics:</strong></td>
<td></td>
</tr>
<tr>
<td><code>show spanning-tree [&lt; port-list &gt;]</code></td>
<td>below</td>
</tr>
<tr>
<td>`show spanning-tree instance &lt; ist</td>
<td>1..16 &gt;`</td>
</tr>
<tr>
<td><strong>MSTP Configuration</strong></td>
<td></td>
</tr>
<tr>
<td><code>show spanning-tree [ port-list ] config</code></td>
<td>6-74</td>
</tr>
<tr>
<td>`show spanning-tree [ port-list ] config instance &lt; ist</td>
<td>1..16 &gt;`</td>
</tr>
<tr>
<td><code>show spanning-tree mst-config</code></td>
<td>6-76</td>
</tr>
<tr>
<td>`show spanning-tree pending&lt; &lt; instance</td>
<td>ist &gt;</td>
</tr>
</tbody>
</table>

Displaying MSTP Statistics

**Displaying Switch Statistics for the Common Spanning Tree.** This command displays the MSTP statistics for the connections between MST regions in a network.

**Syntax:** `show spanning-tree`

*This command displays the switch’s global and regional spanning-tree status, plus the per-port spanning-tree operation at the regional level. Note that values for the following parameters appear only for ports connected to active devices: Designated Bridge, Hello Time, PtP, and Edge.*

**Syntax:** `show spanning-tree < port-list >`

*This command displays the spanning-tree status for the designated port(s). You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks. For example, to display data for port A20-A24 and trk1, you would use this command: show spanning-tree a20-trk1*
Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

Switch-1(config)# show spanning-tree
  Multiple Spanning Tree (MST) Information
  STP Enabled : Yes
  Force Version : MSTP-operation
  IST Mapped VLANs : 1,66
  Switch MAC Address : 0004ea-5e2000
  Switch Priority : 32768
  Max Age : 20
  Max Hops : 20
  Forward Delay : 15
  Topology Change Count : 0
  Time Since Last Change : 2 hours
  CST Root MAC Address : 00022d-47367f
  CST Root Priority : 0
  CST Root Path Cost : 4000000
  CST Root Port : A1
  IST Regional Root MAC Address : 000883-028300
  IST Regional Root Priority : 32768
  IST Regional Root Path Cost : 200000
  IST Remaining Hops : 19

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Cost</th>
<th>Priority</th>
<th>State</th>
<th>Designated Bridge</th>
<th>Hello Time</th>
<th>PtP Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Forwading</td>
<td>000883-028300</td>
<td>9</td>
</tr>
<tr>
<td>A2</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Blocking</td>
<td>0001e7-948300</td>
<td>9</td>
</tr>
<tr>
<td>A3</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Forwarding</td>
<td>000883-02a700</td>
<td>2</td>
</tr>
<tr>
<td>A4</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A5</td>
<td>10/100TX</td>
<td>Auto</td>
<td>128</td>
<td>Disabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>.</td>
<td>.</td>
<td>.</td>
<td>.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 6-28. Example of Common Spanning Tree Status on an MSTP Switch

Switch’s Spanning Tree Configuration and Identity of VLANs Configured in the Switch for the IST Instance
Identifies the overall spanning-tree root for the network.
Lists the switch’s MSTP root data for connectivity with other regions and STP or RSTP devices.
Identifies the spanning-tree root for the IST Instance for the region.
Internal Spanning Tree Data (IST Instance) for the region in which the Switch Operates
Yes means the switch is operating the port as if it is connected to switch, bridge, or end node (but not a hub).
For Edge, No (edge-port operation disabled) indicates the port is configured for connecting to a LAN segment that includes a bridge or switch. Yes indicates the port is configured for a host (end node) link. Refer to the edge-port description under “Configuring Basic Port Connectivity Parameters” on page 6-61.
Displaying Switch Statistics for a Specific MST Instance.

**Syntax:** show spanning-tree instance < ist | 1..16 >

*This command displays the MSTP statistics for either the IST instance or a numbered MST instance running on the switch.*

```
Switch-1(config)# show spanning-tree instance 1

MST Instance Information

  Instance ID : 1
  Mapped VLANs : 11.22
  Switch Priority : 32768
  Topology Change Count : 4
  Time Since Last Change : 6 secs

  Regional Root MAC Address : 0001e7-948300
  Regional Root Priority : 32768
  Regional Root Path Cost : 400000
  Regional Root Port : A1
  Remaining Hops : 18

  Port | Type | Cost | Priority | Role | State     | Bridge
  ---- |------ |----- |----------|------|-----------|---------
       |       |     |          |      |           |         
  A1   | 10/100TX | 200000 | 128     | Root | Forwarding | 000883-028300
  A2   | 10/100TX | 200000 | 128     | Designated | Forwarding | 000883-02a700
  A3   | 10/100TX | 200000 | 112     | Designated | Forwarding | 000883-02a700
  A4   | 10/100TX | Auto | 128     | Disabled | Disabled
  ::   | ::    | ::    | ::      | ::    | ::        | ::
```

*Figure 6-29. Example of MSTP Statistics for a Specific Instance on an MSTP Switch*
Spanning-Tree Operation
802.1s Multiple Spanning Tree Protocol (MSTP)

Displaying the MSTP Configuration

**Displaying the Global MSTP Configuration.** This command displays the switch's basic and MST region spanning-tree configuration, including basic port connectivity settings.

**Syntax:** show spanning-tree config

*The upper part of this output shows the switch's global spanning-tree configuration that applies to the MST region. The port listing shows the spanning-tree port parameter settings for the spanning-tree region operation (configured by the spanning-tree <port-list> command). For information on these parameters, refer to “Configuring Basic Port Connectivity Parameters” on page 6-61.*

**Syntax:** show spanning-tree <port-list> config

*This command shows the same data as the above command, but lists the spanning-tree port parameter settings for only the specified port(s) and/or trunk(s). You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks. For example, to display data for port A20-A24 and trk1, use this command: show spanning-tree a20-trk1 config*
Displaying Per-Instance MSTP Configurations. These commands display the per-instance port configuration and current state, along with instance identifiers and regional root data.

**Syntax:** `show spanning-tree config instance < ist | 1..16 >`

*The upper part of this output shows the instance data for the specified instance. The lower part of the output lists the spanning-tree port settings for the specified instance.*

**Syntax:** `show spanning-tree < port-list > config instance < ist | 1..16 >`

*This command shows the same data as the above command, but lists the spanning-tree port parameter settings for only the specified port(s) and/or trunk(s). You can list data for a series of ports and port trunks by specifying the first and last port or trunk of any consecutive series of ports and trunks. For example, to display data for port A20-A24 and trk1, use this command:*

`show spanning-tree a20-trk1 config instance 1`

---

**Figure 6-31. Example of the Configuration Listing for a Specific Instance**

```
Switch-2(config)# show spanning-tree config instance 1

MST Instance Configuration Information
<table>
<thead>
<tr>
<th>Instance ID</th>
<th>Switch Priority</th>
<th>Mapped VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>32768</td>
<td>11,22</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port Type</th>
<th>Cost</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>A4 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>A5 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A23 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>A24 10/100TX</td>
<td>Auto</td>
<td>128</td>
</tr>
<tr>
<td>Trk1</td>
<td>1000000</td>
<td>128</td>
</tr>
</tbody>
</table>
```

---
Displaying the Region-Level Configuration in Brief. This command output is useful for quickly verifying the allocation of VLANs in the switch's MSTP configuration and for viewing the configured region identifiers.

**Syntax:** show spanning-tree mst-config

*This command displays the switch's regional configuration.*

**Note:** The switch computes the M**STP Configuration Digest** from the VID to MSTI configuration mappings on the switch itself. As required by the 802.1s standard, all MSTP switches within the same region must have the same VID to MSTI assignments, and any given VID can be assigned to either the IST or one of the MSTIs within the region. Thus, the MSTP Configuration Digest must be identical for all MSTP switches intended to belong to the same region. When comparing two MSTP switches, if their Digest identifiers do not match, then they cannot be members of the same region.

```
Switch-2(config)# show spanning-tree mst-config

MST Configuration Identifier Information

MST Configuration Name : REGION_1
MST Configuration Revision : 1
MST Configuration Digest : 0xDAD6A13EC5141980B7EBDA71D8991E7C

IST Mapped VLANs : 1.66
Instance ID Mapped VLANs
------------------------------
1          11.22
2          33.44,55
```

**Figure 6-32. Example of a Region-Level Configuration Display**

Refer to the "Note", above.
Displaying the Pending MSTP Configuration. This command displays the MSTP configuration the switch will implement if you execute the spanning-tree pending apply command (Refer to “Enabling an Entire MST Region at Once or Exchanging One Region Configuration for Another” on page 6-69.)

Syntax:  show spanning-tree pending < instance | mst-config >

instance < 1..16 | ist >

Lists region, instance I.D. and VLAN information for the specified, pending instance.

mst-config

Lists region, IST instance VLAN(s), numbered instances, and assigned VLAN information for the pending MSTP configuration.

```
HPswitch# show spanning-tree pending instance 1
Pending MST Instance Configuration Information

MST Configuration Name : New-Version_01
MST Configuration Revision : 10
Instance ID : 1
Mapped VLANs : 1,22

Switch-1(config)# show spanning-tree pending mst-config
Pending MST Configuration Identifier Information

MST Configuration Name : New-Version_01
MST Configuration Revision : 10

IST Mapped VLANs : 11,33
Instance ID Mapped VLANs
--------- -----------------------------------------------
1 1,22
```

Figure 6-33. Example of Displaying a Pending Configuration
Operating Notes

**SNMP MIB Support for MSTP.** MSTP is a superset of the STP/802.1D and RSTP/802.1w protocols and uses the MIB objects defined for these two protocols. Also, as of December, 2003, there has been no formal MIB definition published for 802.1s MSTP managed objects.

Troubleshooting

**Duplicate packets on a VLAN, or packets not arriving on a LAN at all.** The allocation of VLANs to MSTIs may not be identical among all switches in a region.

**A Switch Intended To Operate Within a Region Does Not Receive Traffic from Other Switches in the Region.** An MSTP switch intended for a particular region may not have the same configuration name or region revision number as the other switches intended for the same region. The MSTP Configuration Name and MSTP Configuration Revision number must be identical on all MSTP switches intended for the same region. Another possibility is that the set of VLANs configured on the switch may not match the set of VLANs configured on other switches in the intended region.
Introduction

Switch meshing is a load-balancing technology that enhances reliability and performance in these ways:

- Provides significantly better bandwidth utilization than either Spanning Tree Protocol (STP) or standard port trunking.
- Uses redundant links that remain open to carry traffic, removing any single point of failure for disabling the network, and allowing quick responses to individual link failures. This also helps to maximize investments in ports and cabling.
- Unlike trunked ports, the ports in a switch mesh can be of different types and speeds. For example, a 10Base-FL port and a 1GB port can be included in the same switch mesh.

![Figure 7-1. Example of Switch Meshing](image-url)
Finding the Fastest Path. Using multiple switches redundantly linked together to form a *meshed switch domain*, switch meshing dynamically distributes traffic across load-balanced switch paths by seeking the fastest paths for new traffic between nodes. In actual operation, the switch mesh periodically determines the best (lowest latency) paths, then assigns these paths as the need arises. The path assignment remains until the related MAC address entry times out. The mesh sees later traffic between the same nodes as new traffic, and may assign a different path, depending on conditions at the time. For example, at one time the best path from node A to node B is through switch 2. However, if traffic between node A and node B ceases long enough for the path assignment to age out, then the next time node A has traffic for node B, the assigned path between these nodes may be through switch 3 if network conditions have changed significantly.

**Note**

The *mac-age-time* parameter determines how long an inactive path assignment remains in memory. Refer to “System Information” in the chapter titled “Interface Access, System Information, and Friendly Port Names” in the *Management and Configuration Guide* for your switch.

Because Redundant Paths Are Active, Meshing Adjusts Quickly to Link Failures. If a link in the mesh fails, the fast convergence time designed into meshing typically has an alternate route selected in less than a second for traffic that was destined for the failed link.

Meshing Allows Scalable Responses to Increasing Bandwidth Demand. As more bandwidth is needed in a LAN backbone, another switch and another set of links can be added. This means that bandwidth is not limited by the number of trunk ports allowed in a single switch.

**Meshing Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>viewing a mesh configuration</td>
<td>n/a</td>
<td>7-10</td>
<td>7-14</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuring a Switch Mesh</td>
<td>n/a</td>
<td>7-10</td>
<td>7-17</td>
<td>n/a</td>
</tr>
<tr>
<td>Backwards Compatibility Mode</td>
<td>Disabled</td>
<td>n/a</td>
<td>7-17</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Switch Meshing Fundamentals

Terminology

**Switch Mesh Domain.** This is a group of meshed switch ports exchanging meshing protocol packets. Paths between these ports can have multiple redundant links without creating broadcast storms.

![Diagram of Switch Mesh Domain in a Network](image)

**Figure 7-2. Example of a Switch Mesh Domain in a Network**

**Edge Switch.** This is a switch that has some ports in the switch meshing domain and some ports outside of the domain. (See figure 7-2, above.)
Operating Rules

(See also “Requirements and Restrictions” on page 7-24.)

- A meshed switch can have some ports in the meshed domain and other ports outside the meshed domain. That is, ports within the meshed domain must be configured for meshing, while ports outside the meshed domain must not be configured for meshing.
- Meshed links must be point-to-point switch links.
- On any switch, all meshed ports belong to the same mesh domain.
- A switch can have up to 24 meshed ports.
- A mesh domain can include up to 12 switches.
- Up to five interswitch, meshed hops are allowed in the path connecting two nodes through a switch mesh domain. A path of six or more meshed hops between two nodes is unusable. However, in most mesh topologies, there would normally be a shorter path available, and paths of five hops or fewer through the same mesh will continue to operate.
- Hub links between meshed switch links are not allowed.
- If the switch has multiple static VLANs and you configure a port for meshing, the port becomes a tagged member of all such VLANs. If you remove a port from meshing, it becomes an untagged member of only the default VLAN.
- A port configured as a member of a static trunk (LACP, FEC, or Trunk) cannot also be configured for meshing.
- If a port belongs to a dynamic LACP trunk and you impose meshing on the port, it automatically ceases to be a member of the dynamic trunk.
- Meshing is not supported on ports with 802.1x port access security.
- On a port configured for meshing, if you subsequently remove meshing from the port’s configuration and reboot the switch, the port returns to its default configuration. (It does not revert to any non-default configuration it had before being configured for meshing).
- Switches from the same product families must run the same version of the OS. For example, if one Series 5300XL switch has an OS update, then any other Series 5300XL switches in the mesh must be updated. HP recommends that you always use the most recent version of the OS.
- If meshing is configured on the switch, the routing features (IP routing, RIP, and OSPF) must be disabled. That is, the switch’s meshing and routing features cannot be enabled at the same time.
- Spanning tree must be the same for all switches in the mesh (enabled or disabled). If spanning tree is enabled in the mesh, it must be the same version on all switches in the mesh (STP or RSTP).
If a switch in the mesh has GVRP enabled, then all switches in the mesh must have GVRP enabled. Otherwise, traffic on a dynamic VLAN may not pass through the mesh.

If a switch in the mesh has a particular static vlan configured, then all switches in the mesh must have that static vlan configured.

If a switch in the mesh has IGMP enabled, then all switches in the mesh must have IGMP enabled.

If a switch in the mesh has CDP enabled, then all switches in the mesh must have CDP enabled.

After adding or removing a port from the mesh, you must save the current configuration and reboot the switch in order for the change to take effect.

Multiple meshed domains require separation by either a non-meshed switch or a non-meshed link. For example:

Figure 7-3. Example of Multiple Meshed Domains Separated by a Non-Mesh Switch or a Non-Mesh Link

- If GVRP is enabled, meshed ports in a switch become members of any dynamic VLANs created in the switch in the same way that they would if meshing was not configured in the switch. (For more on GVRP, refer to “GVRP” on page 3-1.)
Switch Meshing
Switch Meshing Fundamentals

GVRP Note

HP Procurve 1600M/2400M/2424M/4000M/8000M switches do not offer the GVRP feature. If any of these switches are in your switch mesh, then GVRP must be disabled on any Series 5300XL switches in the mesh.

Note

- A switch mesh domain (figure 7-1 on page 7-2) cannot include either a switch that is not configured for meshing, or a hub.
- Where a given pair of switches are linked with meshed ports, you must not also link the pair together through non-meshed ports unless you have also enabled STP or RSTP to prevent a loop from forming.

![Figure 7-4. Example of an Unsupported Topology]

- The switch blocks traffic on a meshed port connected to a non-meshed port on another switch.
- Switch meshing does not allow trunked links (FEC, LACP, or Trunk) between meshed ports.

Linking a non-mesh device or port into the mesh causes the meshed switch port(s) connected to that device to shut down.

Backward Compatibility Note

The HP ProCurve Series 5300XL switches can interoperate with older devices in a switch mesh only after being placed in backwards compatibility mode. This is done with the `mesh backward-comp` command.

Using a Heterogeneous Switch Mesh

You can use Series 5300XL switches together with any of the older HP Procurve Switch 1600M/2400M/2424M/4000M/8000M models. These restrictions also apply:
Switch Meshing
Switch Meshing Fundamentals

- All Series 5300XL switches in the mesh must be placed in backward compatible mode. This is done with the `mesh backward-compat` command.
- The older models cannot be used in a mesh environment with Series 5300XL switches where there is a duplicate MAC address on multiple switches and different VLANs. If you add an older model switch in this environment after the mesh is established, this switch will not be admitted to the mesh. If an older model switch is operating in a mesh with Series 5300XL switches and you introduce a topology that creates a duplicate MAC address on multiple switches, the device accessed by these multiple switches will be blocked. For example:

**Scenario 1:** In a heterogeneous mesh, creating the mesh with only one Series 5300XL switch connected to the host (on VLAN 1, for example), and then connecting a second Series 5300XL switch to the host (regardless of the VLAN used) results in connectivity issues with the host.

**Scenario 2:** Adding the Switch 4000M after bringing up the mesh with two Series 5300XL switches already connected to the host as shown here (with or without separate VLANs) blocks the Switch 4000M from the mesh.

![Diagram of unsupported topology](image)

**Figure 7-5. Example of an Unsupported Heterogeneous Topology Where Duplicate MAC Addresses Come Through Different Switches (Regardless of the VLANs Used)**
Creating the mesh with only one Series 5300XL switch connected to the host, and using tagged VLANs for multiple connections between the host and the meshed switch allows normal meshing operation.

The Switch 4000M is not supported in topologies allowing the same MAC address on multiple switches.

**Figure 7-6. Example of a Supported Heterogeneous Topology Where Duplicate MAC Addresses Come Through Different VLANs on the Same Switch**

Note that in figures 7-5 and 7-6, if all switches are Series 5300XL switches, then you can use either topology.

Also, if you have two separate switch meshes with the topology shown in figure 7-7, you cannot join them into a single mesh.

**Figure 7-7. Example of Topology Where Adjacent Switch Meshes Cannot Be Merged Into a Single Mesh**

- Automatic Broadcast Control (ABC) on HP Procurve 8000M/4000M/2424M/2400M/1600M switches is not supported when these switches are used in the same mesh domain with Series 5300XL switches. Thus, in a mesh domain populated with both types of switches, ABC must be disabled (the default setting) on all of the 8000M/4000M/2424M/2400M/1600M switches in the domain.
Bringing Up a Switch Mesh Domain:

When a meshed port detects a non-meshed port on the opposite end of a point-to-point connection, the link will be blocked. Thus, as you bring up switch meshing on various switches, you may temporarily experience blocked ports where meshed links should be running. These conditions should clear themselves after all switches in the mesh have been configured for meshing and their switches rebooted. To reduce the effect of blocked ports during bring-up, configure meshing and reboot the switches before installing the meshed switches in the network.

Further Operating Information

Refer to “Operating Notes for Switch Meshing” on page 7-18.

Configuring Switch Meshing

Preparation

Before configuring switch meshing:

- Review the Operating Rules (page 7-5), and particularly the restrictions and requirements for using switch meshing in environments that include static trunks, multiple static VLANs, GVRP, IGMP, and STP.
- To avoid unnecessary system disruption, plan the mesh bring-up to minimize temporary port-blocking. (Refer to “Bringing Up a Switch Mesh Domain:” on page 7-10.)
- To view the current switch mesh status on the Series 5300XL switches, use the CLI `show mesh` command (page 7-14).

Menu: To Configure Switch Meshing

1. From the Main Menu, select:
   
   2. Switch Configuration
      
      2. Port/Trunk Settings

2. Press [E] (for Edit) to access the load balancing parameters.
Figure 7-8. Example of the Screen for Configuring Ports for Meshing

3. In the Group column, move the cursor to the port you want to assign to the switch mesh.


5. Use the **up-arrow or down-arrow** key to select the next port you want to include in your mesh domain, then press [M] again. For example, if you were adding ports A1 and A2 to your mesh domain, the screen would appear similar to figure 7-9:
Switch Meshing
Configuring Switch Meshing

---

**Configuring Switch Meshing**

Ports A1 and A2 configured for meshing.

Figure 7-9. Example of Mesh Group Assignments for Several Ports

6. Repeat step 5 for all ports you want in the mesh domain.

**Notes**

For meshed ports, leave the **Type** setting blank. (Meshed ports do not accept a **Type** setting.)

All meshed ports in the switch automatically belong to the same mesh domain. (See figure 7-2 on page 7-4.)

7. When you finish assigning ports to the switch mesh, press **[Enter]**, then **[S]** (for **Save**). You will then see the following screen.
The asterisk indicates that you must reboot the switch to cause the Mesh configuration change to take effect.

---

**Figure 7-10. After Saving a Mesh Configuration Change, Reboot the Switch**

8. Press [0] to return to the Main menu.

9. To activate the mesh assignment(s) from the Main menu, reboot the switch by pressing the following keys:
   a. [6] (for **Reboot Switch**)
   b. Space bar (to select **Yes**).
   c. 13 (to start the reboot process).

(The switch cannot dynamically reconfigure ports to enable or disable meshing, so it is always necessary to reboot the switch after adding or deleting a port in the switch mesh.)
Switch Meshing
Configuring Switch Meshing

CLI: To View and Configure Switch Meshing

Port Status and Configuration Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>viewing switch mesh status</td>
<td>n/a</td>
<td>n/a</td>
<td>below</td>
<td>n/a</td>
</tr>
<tr>
<td>configuring switch meshing</td>
<td>Disabled</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Viewing Switch Mesh Status

Syntax: show mesh

Lists the switch ports configured for meshing, along with the State of each mesh-configured connection, the MAC address of the switch on the opposite end of the link (Adjacent Switch), and the MAC address of the port on the opposite end of the link (Peer Port).

Reading the Show Mesh Output. For each port configured for meshing, the State column indicates whether the port has an active link to the mesh or is experiencing a problem. The status of the backwards compatibility option is also displayed. For more details on the backwards compatibility option see “CLI: Configuring Switch Meshing” on page 7-17

Figure 7-11. Example of the Show Mesh Report
Table 7-1. State Descriptions for Show Mesh Output

<table>
<thead>
<tr>
<th>State</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Established</td>
<td>The port is linked to a meshed port on another switch and meshing traffic is flowing across the link. The show mesh listing includes the MAC addresses of the adjacent switch and direct connection port on the adjacent switch.</td>
</tr>
<tr>
<td>Not Established</td>
<td>The port may be linked to a switch on a port that is not configured for meshing or has gone down.</td>
</tr>
<tr>
<td>Initial</td>
<td>The port has just come up as a meshed port and is trying to negotiate meshing.</td>
</tr>
<tr>
<td>Disabled</td>
<td>The port is configured for meshing but is not connected to another device.</td>
</tr>
<tr>
<td>Error</td>
<td>Indicates a multiple MAC-address error. This occurs when you have two or more mesh ports from the same switch linked together through a hub.</td>
</tr>
<tr>
<td>Topology Error</td>
<td>Two meshed switches are connected via a hub, and traffic from other, non-meshed devices, is flowing into the hub. The show mesh listing includes the MAC addresses of the adjacent switch and direct connection port on the adjacent switch.</td>
</tr>
</tbody>
</table>

Topology Example with Show Mesh. Suppose that you have the following topology:

![Diagram of meshed topology](image)

The links from ports C1 and D1 are valid meshed links. All other links are invalid for meshing. Figure 7-13 on page 7-16 demonstrates the show mesh listing for this topology.

Figure 7-12. Example of a Meshed Topology with Some Mesh Ports Incorrectly Linked

Table 7-2 on page 7-16 describes the meshing operation in the above topology.
Table 7-2. Operating Details for Figure 7-12

<table>
<thead>
<tr>
<th>Port</th>
<th>Meshing?</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Yes</td>
<td>Connected to a port that may not be configured for meshing</td>
</tr>
<tr>
<td>A2</td>
<td>Yes</td>
<td>Connected to a switch port on a device that is not configured for meshing (another switch, or a hub). In this case, the Topology Error message indicates that the switch detects a meshed port on another, non-adjacent device that is also connected to the non-meshed switch or hub. However, meshing will not operate properly through this connection.</td>
</tr>
<tr>
<td>B1</td>
<td>Yes</td>
<td>Not connected to another device.</td>
</tr>
<tr>
<td>C1</td>
<td>Yes</td>
<td>Connected to a meshed port on the same adjacent switch as D1 with meshing operating properly.</td>
</tr>
<tr>
<td>D1</td>
<td>Yes</td>
<td>Connected to a meshed port on the same adjacent switch as C1 with meshing operating properly.</td>
</tr>
</tbody>
</table>

Figure 7-13 lists the show mesh display for the topology and meshing configuration in figure 7-12:

```
HPSwitch# show mesh

Status and Counters - Switch Mesh Information

Backward Compatibility mode enabled : No

+-----+-----------------+-----------------+-----------------+
| Port | State           | Adjacent Switch | Peer Port       |
+-----+-----------------+-----------------+-----------------+
| A1   | Not Established | 0060b0-889e00   | 0060b0-889e7b   |
| A2   | Topology Error  | 0060b0-889e00   | 0060b0-889e7a   |
| B1   | Disabled        | 0060b0-889e00   | 0060b0-889e7a   |
| C1   | Established     | 0060b0-889e00   | 0060b0-889e79   |
| D1   | Established     | 0060b0-889e00   | 0060b0-889e79   |
```

Figure 7-13. Example of the Show Mesh Listing for the Topology in Figure 7-12
CLI: Configuring Switch Meshing

**Syntax:**

```
[no] mesh [e] < port-list >
```

Enables or disables meshing operation on the specified ports.

```
[no] mesh backward-compat
```

Enables or disables the switch for backward compatible mode. This allows the Series 5300XL switches to interoperate with earlier switch models in the same switch mesh.

**Note:** Enabling this mode turns off some configuration checking done in a mesh with only Series 5300XL switches. This command does not require a reboot to take effect.

All meshed ports on a switch belong to the same mesh domain. Thus, to configure multiple meshed ports on a switch, you need to:

1. Specify the ports you want to operate in the mesh domain.
2. Use **write memory** to save the configuration to the startup-config file.
3. Reboot the switch

For example, to configure meshing on ports A1-A4, B3, C1, and D1-D3:

```
HPswitch(config)# mesh e a1-a4,b3,c1,d1-d3
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

**Figure 7-14. Example of How To Configure Ports for Meshing**

To remove a port from meshing, use the "no" version of **mesh**, followed by **write memory** and rebooting the switch. For example, to remove port C1 from the mesh:

```
HPswitch# config
HPswitch(config)# no mesh c1
Command will take effect after saving configuration and reboot.
HPswitch(config)# write memory
HPswitch(config)# boot
Device will be rebooted, do you want to continue [y/n]? y
```

**Figure 7-15. Example of Removing a Port from the Mesh**
Operating Notes for Switch Meshing

In a switch mesh domain traffic is distributed across the available paths with an effort to keep latency the same from path to path. The path selected at any time for a connection between a source node and a destination node is based on these latency and throughput cost factors:

- Outbound queue depth, or the current outbound load factor for any given outbound port in a possible path
- Port speed, such as 10Mbps versus 100Mbps; full-duplex or half-duplex
- Inbound queue depth, or how busy is a destination switch in a possible path
- Increased packet drops, indicating an overloaded port or switch

Paths having a lower cost will have more traffic added than those having a higher cost. Alternate paths and cost information is discovered periodically and communicated to the switches in the mesh domain. This information is used to assign traffic paths between devices that are newly active on the mesh. This means that after an assigned path between two devices has timed out, new traffic between the same two devices may take a different path than previously used.

To display information on the operating states of meshed ports and the identities of adjacent meshed ports and switches, see “Viewing Switch Mesh Status” on page 7-14.

Flooded Traffic

Broadcast and multicast packets will always use the same path between the source and destination edge switches unless link failures create the need to select new paths. (Broadcast and multicast traffic entering the mesh from different edge switches are likely to take different paths.) When an edge switch receives a broadcast from a non-mesh port, it floods the broadcast out all its other non-mesh ports, but sends the broadcast out only those ports in the mesh that represent the path from that edge switch through the mesh domain. (Only one copy of the broadcast packet gets to each edge switch for broadcast out of its nonmeshed ports. This helps to keep the latency for these packets to each switch as low as possible.)
Any mesh switches that are not edge switches will flood the broadcast packets only through ports (paths) that link to separate edge switches in the controlled broadcast tree. The edge switches that receive the broadcast will flood the broadcast out all non-meshed ports. Some variations on broadcast/multicast traffic patterns, including the situation where multiple VLANs are configured and a broadcast path through the mesh domain leads only to ports that are in the same VLAN as the device originating the broadcast.

Unicast Packets with Unknown Destinations

A meshed switch receiving a unicast packet with an unknown destination does not flood the packet onto the mesh. Instead, the switch sends a query on the mesh to learn the location of the unicast destination. The meshed switches then send 802.2 test packets through their non-meshed ports. After the unicast destination is found and learned by the mesh, subsequent packets having the same destination address will be forwarded. By increasing the \textbf{MAC Age Time} you can cause the switch address table to retain device addresses longer. (For more on \textbf{MAC Age Time}, refer to “System Information” in the chapter titled “Interface Access, System Information, and Friendly Port Names” in the \textit{Management and Configuration Guide} for your switch.) Because the switches in a mesh exchange address information, this will help to decrease the number of unicast packets with unknown destinations, which improves latency within the switch mesh. Also, in an IP environment, HP recommends that you configure IP addresses on meshed switches. This makes the discovery mechanism more robust, which contributes to decreased latency.
Spanning Tree Operation with Switch Meshing

Using STP or RSTP with several switches and no switch meshing configured can result in unnecessarily blocking links and reducing available bandwidth. For example:

![Diagram showing STP enabled and creating traffic bottlenecks vs. enabling meshing on links between switch ports removes STP blocks on meshed redundant links.](image)

**Problem:**
STP enabled and creating traffic bottlenecks.

**Solution:**
Enabling meshing on links between switch ports removes STP blocks on meshed redundant links.

**Figure 7-17. Example Using STP Without and With Switch Meshing**

If you enable STP or RSTP on any meshed switch, you should enable either STP or RSTP on all switches in the mesh. (That is, if you are going to use spanning-tree in a switch mesh, all switches in the mesh should be configured with the same type of spanning-tree: 802.1d/STP or 802.1w/RSTP.) STP and RSTP see a meshed domain as a single link. However, on edge switches in the domain, STP and RSTP will manage non-meshed redundant links from other devices. For example:
**Note on RSTP edge-port mode**

When using RSTP and interconnecting Series 5300XL switches in a mesh with switches that are not in the mesh, all the non-mesh switch ports (as indicated in the figure above) should have the parameter edge-port set to FALSE. For more information on RSTP edge-port parameter see “Optimizing the RSTP Configuration” on page 6-11.

STP or RSTP should be configured on non-mesh devices that use redundant links to interconnect with other devices or with multiple switch mesh domains. For example:

In the above case of multiple switch meshes linked with redundant trunks there is the possibility that STP or RSTP will temporarily block a mesh link. This is because it is possible for STP or RSTP to interpret the cost on an external trunked link to be less than the cost on a meshed link. However, if
this condition occurs, the meshed switch that has a blocked link will automatically increase the cost on the external (non-meshed) link to the point where STP or RSTP will block the external link and unblock the meshed link. This process typically resolves itself in approximately 30 seconds.

**Caution**

Spanning tree interprets a switch mesh as a single link. Because the switch automatically gives faster links a higher priority, the default STP or RSTP parameter settings are usually adequate for spanning tree operation. Also, because incorrect STP or RSTP settings can adversely affect network performance, you should not make changes unless you have a strong understanding of how spanning tree operates.

In a mesh environment, the default RSTP timer settings (**Hello Time** and **Forward Delay**) are usually adequate for RSTP operation. Because a packet crossing a mesh may traverse several links within the mesh, using smaller-than-default settings for the RSTP Hello Time and Forward Delay timers can cause unnecessary topology changes and end-node connectivity problems.

For more on STP and RSTP, refer to chapter 13, “802.1w Rapid Spanning Tree Protocol (RSTP) and 802.1d Spanning Tree Protocol”. Also, you may want to examine the IEEE 802.1d or 802.1w standard, depending on which version of spanning-tree you are using.

**Filtering/Security in Meshed Switches**

Because paths through the mesh can vary with network conditions, configuring filters on meshed ports can create traffic problems that are difficult to predict, and is not recommended. However, configuring filters on nonmeshed ports in an edge switch provides you with control and predictability.

**IP Multicast (IGMP) in Meshed Switches**

Like trunked ports, the switch mesh domain appears as a single port to IGMP. However, unlike trunked ports, IGMP protocol and multicast traffic may be sent out over several links in the mesh in the same manner as broadcast packets.

**Static VLANs**

In a network having a switch mesh domain and multiple static VLANs configured, all static VLANs must be configured on each meshed switch, even if no ports on the switch are assigned to any VLAN. (The switch mesh is a member of all static VLANs configured on the switches in the mesh.)
When static VLANs are configured, the mesh is seen as a single entity by each VLAN. All ports in the mesh domain are members of all VLANs and can be used to forward traffic for any VLAN. However, the non-mesh ports on edge switches that allow traffic to move between the mesh and non-meshed devices belong to specific VLANs and do not allow packets originating in a specific VLAN to enter non-meshed devices that do not belong to that same VLAN. (It is necessary to use a router to communicate between VLANs.) For example, in the following illustration, traffic from host A entering the switch mesh can only exit the mesh at the port for hosts B and E. Traffic from host A for any other host (such as C or D) will be dropped because only hosts B and E are in the same VLAN as host A.

**Figure 7-20. VLAN Operation with a Switch Mesh Domain**

**Dynamic VLANs**

If GVRP is enabled, meshed ports in a switch become members of any dynamic VLANs created in the switch in the same way that they would if meshing was not configured in the switch. (For more on GVRP, refer to “GVRP” on page 3-1.)
Requirements and Restrictions

- **Supported Mesh Domain Size:**
  - In a *partially interconnected* mesh domain, where there is not a direct connection from every meshed switch to every other meshed switch, the recommended maximum is 12 switches. Figure 7-21 shows a meshed backbone with the maximum supported switch count in a partially interconnected mesh domain.
  - In a *fully interconnected* mesh domain, where there is a direct connection from every meshed switch to every other meshed switch, the recommended maximum is five switches. Figure 7-22 shows a fully interconnected mesh.

![Figure 7-21. Example of a Partially Interconnected Mesh with the Maximum Recommended Switch Count](image1)

![Figure 7-22. Example of a Fully Interconnected Mesh with the Maximum Switch Count](image2)
Mesh Support Within the Domain: All switches in the mesh domain, including edge switches, must support the HP switch meshing protocol.

Switch Hop Count in the Mesh Domain: A maximum of five (meshed) switch hops is allowed in the path connecting two nodes in a switch mesh domain. A path of six meshed hops is unusable. However, this does not interfere with other, shorter paths in the same domain.

Connecting Mesh Domains: To connect two separate switch meshing domains, you must use non-meshed ports. (The non-meshed link can be a port trunk or a single link.) Refer to figure 7-3 on page 7-6.

Fast EtherChannel® (FEC): This cannot be configured on a meshed port. (You can configure FEC on non-meshed ports in a switch that also has meshed ports.)

Multiple Links Between Meshed Switches: Multiple mesh ports can be connected between the same two switches, to provide higher bandwidth. Each port that you want in the mesh domain should be configured as Mesh (and not as a trunk—Trk). Note that if you configure a port as Mesh, there is no “Type” selection for that port.

Automatic Broadcast Control: Series 5300XL switches do not offer this feature. Thus, in a switch mesh comprised of Series 5300XL switches and any of the 1600M/2400M/2424M/4000M/8000M switches, ABC must be disabled (the default setting) on the 1600M/2400M/2424M/4000M/8000M switches.

Network Monitor Port: If a network monitor port is configured, broadcast packets may be duplicated on this port if more than one port is being monitored and switch meshing is enabled.

Compatibility with Older Switches: Only after the Series 5300XL switch is placed in backwards compatibility mode will it operate with older switches. For more information see “CLI: Configuring Switch Meshing” on page 7-17. Each entry in a Series 5300XL switch MAC-address table consists of a MAC address and a VLAN ID (VID). In older switches there is no VID; just a MAC address. The older switches will therefore see indistinguishable, duplicate addresses where the Series 5300XL switches will see multiple different addresses consisting of the same MAC address and different VIDs. In a switch mesh that includes any 1600M/2400M/2424M/4000M/8000M switches, duplicate MAC addresses entering the mesh on different switches are not allowed. (These older switches do not recognize multiple instances of a particular MAC address on different VLANs.) If you try to add one of these switches to a mesh comprised entirely of Series 5300XL switches, and any of the Series 5300XL switches detects a duplicate MAC address entering the mesh through separate switches, the 1600M/2400M/2424M/4000M/8000M switch will not be allowed in the switch mesh.
(See also “Operating Rules” on page 7-5.)

For additional information on troubleshooting meshing problems, refer to “Using a Heterogeneous Switch Mesh” on page 7-7 and "Mesh-Related Problems" in appendix C, "Troubleshooting" of the Management and Configuration Guide for your switch.
Quality of Service (QoS): Managing Bandwidth More Effectively

Contents

**Introduction** ......................................................... 8-2
  Terminology ......................................................... 8-5
  Overview ............................................................... 8-6
  Classifiers for Prioritizing Outbound Packets ............ 8-8

**Preparation for Configuring QoS** ........................................ 8-11

**Using QoS Classifiers To Configure Quality of Service for Outbound Traffic** ........................................ 8-13
  QoS UDP/TCP Priority .................................................. 8-13
  QoS IP-Device Priority ............................................... 8-19
  QoS IP Type-of-Service (ToS) Policy and Priority ........ 8-24
  QoS LAN Protocol Priority ........................................... 8-36
  QoS VLAN-ID (VID) Priority ........................................ 8-38
  QoS Source-Port Priority ............................................ 8-43
  Differentiated Services Codepoint (DSCP) Mapping .... 8-50
  Note On Changing a Priority Setting ...................... 8-53

**Configuring QoS from the Web Browser Interface** ................. 8-56

**IP Multicast (IGMP) Interaction with QoS** ......................... 8-57

**QoS Messages in the CLI** .............................................. 8-57

**QoS Operating Notes** .................................................. 8-58
Introduction

As the term suggests, network policy refers to the network-wide controls you can implement to:

- Ensure uniform and efficient traffic handling throughout your network, while keeping the most important traffic moving at an acceptable speed, regardless of current bandwidth usage.
- Exercise control over the priority settings of inbound traffic arriving in and travelling through your network.

Adding bandwidth is always a good idea, but it is not always feasible and does not completely eliminate the potential for network congestion. There will always be points in the network where multiple traffic streams merge or where network links will change speed and capacity. The impact and number of these congestion points will increase over time as more applications and devices are added to the network.

When (not if) network congestion occurs, it is important to move traffic on the basis of relative importance. However, without Quality of Service (QoS) prioritization, less important traffic can consume network bandwidth and slow down or halt the delivery of more important traffic. That is, without QoS, most traffic received by the switch is forwarded with the same priority it had upon entering the switch. In many cases, such traffic is “normal” priority and competes for bandwidth with all other normal-priority traffic, regardless of its relative importance to your organization’s mission.

This section gives an overview of QoS operation and benefits, and describes how to configure QoS in the console interface.
Quality of Service is a general term for classifying and prioritizing traffic throughout a network. That is, QoS enables you to establish an end-to-end traffic priority policy to improve control and throughput of important data. You can manage available bandwidth so that the most important traffic goes first. For example, you can use Quality of Service to:

- Upgrade or downgrade traffic from various servers.
- Control the priority of traffic from dedicated VLANs or applications.
- Change the priorities of traffic from various segments of your network as your business needs change.
- Set priority policies in edge switches in your network to enable traffic-handling rules across the network.

**Figure 8-1. Example of 802.1p Prioritization Based on CoS Types and Use of Tagged VLANs**

At the edge switch, QoS classifies certain traffic types and in some cases applies a DSCP policy. At the next hop (downstream switch) QoS honors the policies established at the edge switch. Further downstream, another switch may reclassify some traffic by applying new policies, and yet other downstream switches can be configured to honor the new policies.

**Figure 8-2. Example Application of Differentiated Services Codepoint (DSCP) Policies**
Quality of Service (QoS): Managing Bandwidth More Effectively

Introduction

QoS is implemented in the form of rules or policies that are configured on the switch. While you can use QoS to prioritize only the outbound traffic moving through the switch, you derive the maximum benefit by using QoS in an 802.1Q VLAN environment (with 802.1p priority tags) or in an untagged VLAN environment (with DSCP policies) where QoS can set priorities that downstream devices can support without re-classifying the traffic.

By prioritizing traffic, QoS supports traffic growth on the network while optimizing the use of existing resources—and delaying the need for further investments in equipment and services. That is, QoS enables you to:

- Specify which traffic has higher or lower priority, regardless of current network bandwidth or the relative priority setting of the traffic when it is received on the switch.
- Change (upgrade or downgrade) the priority of outbound traffic.
- Override “illegal” packet priorities set by upstream devices or applications that use 802.1Q VLAN tagging with 802.1p priority tags.
- Avoid or delay the need to add higher-cost NICs (network interface cards) to implement prioritizing. (Instead, control priority through network policy.)

QoS on the Series 5300XL switches supports these types of traffic marking:

- **802.1p prioritization**: Controls the outbound port queue priority for traffic leaving the switch, and (if traffic exits through a tagged VLAN) sends the priority setting with the individual packets to the downstream devices.

- **IP Type-of-Service (ToS)**: Enables the switch to set, change, and honor prioritization policies by using the Differentiated Services (diffserv) bits in the ToS byte of IPv4 packet headers.
## Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Use in This Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>codepoint</td>
<td>Refer to DSCP, below.</td>
</tr>
<tr>
<td>downstream device</td>
<td>A device linked directly or indirectly to an outbound switch port. That is, the switch sends traffic to downstream devices.</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Codepoint. (Also termed codepoint) A DSCP is comprised of the upper six bits of the ToS (Type-of-Service) byte in IP packets. There are 64 possible codepoints. In the switch’s default QoS configuration, some codepoints are configured with default 802.1p priority settings for Assured-Forwarding and Expedited Forwarding, while others are unused (and listed with No-override for a priority).</td>
</tr>
<tr>
<td>DSCP policy</td>
<td>A DSCP configured with a specific 802.1p priority (0-7). (Default: No-override). Using a DSCP policy you can configure the switch to assign priority to IP packets. That is, for an IP packet identified by the specified classifier, you can assign a new DSCP and an 802.1p priority (0-7). For more on DSCP, refer to “Details of QoS IP Type-of-Service” on page 8-33. For the DSCP map, see figure 8-18 on page 8-34.</td>
</tr>
<tr>
<td>edge switch</td>
<td>In the QoS context, this is a switch that receives traffic from outside the LAN and forwards it to devices within the LAN. Typically, an edge switch is used with QoS to recognize packets based on classifiers such as TCP/UDP application type, IP-device (address), Protocol (LAN), VLAN-ID (VID), and Source-Port (although it can also be used to recognize packets on the basis of ToS bits). Using this packet recognition, the edge switch can be used to set 802.1p priorities or DSCP policies that downstream devices will then honor.</td>
</tr>
<tr>
<td>inbound port</td>
<td>Any port on the switch through which traffic enters the switch.</td>
</tr>
<tr>
<td>IPv4</td>
<td>Version 4 of the IP protocol.</td>
</tr>
<tr>
<td>outbound packet</td>
<td>A packet leaving the switch through any LAN port.</td>
</tr>
<tr>
<td>outbound port</td>
<td>Any port on the switch through which traffic leaves the switch.</td>
</tr>
<tr>
<td>outbound port queue</td>
<td>For any port, a buffer that holds outbound traffic until it can leave the switch through that port. There are four outbound queues for each port in the switch: high, medium, normal, and low. Traffic in a port’s high priority queue leaves the switch before any traffic in the port’s medium priority queue, and so-on.</td>
</tr>
<tr>
<td>IP-precedence bits</td>
<td>The upper three bits in the Type of Service (ToS) field of an IP packet.</td>
</tr>
<tr>
<td>upstream device</td>
<td>A device linked directly or indirectly to an inbound switch port. That is, the switch receives traffic from upstream devices.</td>
</tr>
<tr>
<td>802.1p priority-</td>
<td>A traffic priority setting carried by packets moving from one device to another in an 802.1Q tagged VLAN environment. This setting can be from 0 - 7. The switch handles an outbound packet on the basis of its 802.1p priority. However, if the packet leaves the switch through an untagged VLAN, this priority is dropped, and the packet arrives at the next, downstream device without an 802.1p priority assignment.</td>
</tr>
<tr>
<td>802.1Q tagged VLAN</td>
<td>A virtual LAN (VLAN) that complies with the 802.1Q standard and is configured as “tagged”. In this environment, IP packets carry an 802.1p priority from one device to the next.</td>
</tr>
</tbody>
</table>
Overview

QoS settings operate on two levels:

- **Controlling the priority of outbound packets moving through the switch:** Each switch port has four outbound traffic queues; “low”, “normal”, “medium”, and “high” priority. Packets leave the switch port on the basis of their queue assignment and whether any higher queues are empty:

<table>
<thead>
<tr>
<th>Port Queue</th>
<th>Priority for Exiting From the Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>High (6 - 7)</td>
<td>First</td>
</tr>
<tr>
<td>Medium (4 - 5)</td>
<td>Second</td>
</tr>
<tr>
<td>Normal (0, 3)</td>
<td>Third</td>
</tr>
<tr>
<td>Low (1 - 2)</td>
<td>Fourth</td>
</tr>
</tbody>
</table>

A QoS configuration enables you to set the outbound priority queue to which a packet is sent. (In an 802.1Q tagged VLAN environment, if QoS is not configured on the switch, but is configured on an upstream device, the priorities carried in the packets determine the forwarding queues in the switch.)

- **Configuring a priority for outbound packets and a service (priority) policy for use by downstream devices:**
  
  - **DSCP Policy:** This feature enables you to set a priority policy in outbound IP packets. (You can configure downstream devices to read and use this policy.) This method is not dependent on tagged VLANs to carry priority policy to downstream devices, and can:
    - Change the codepoint (the upper six bits) in the TOS byte.
    - Set a new 802.1p priority for the packet.

    (Setting DSCP policies requires IPv4 inbound packets. Refer to the “IPv4” entry under “Terminology” on page 8-5.)

  - **802.1p Priority:** If an outbound packet is in an 802.1Q tagged VLAN environment (that is, if the packet is assigned to a tagged VLAN on the outbound port), then the packet carries an 802.1p priority setting that was configured in the switch. This priority setting ranges from 0 to 7, and can be used by downstream devices having up to eight outbound port queues. Thus, while packets within the switch move at the four priority levels shown in table 8-1, above, they still can carry an 802.1p priority that can be used by downstream devices having more or less than the four priority levels in the Series 5300XL switches. Also, if the packet enters the switch with an 802.1p priority setting, QoS can override this setting if configured to do so.
If you are not using multiple tagged VLANs in your network, you can still use the tagged VLAN feature by configuring the default VLAN as a tagged VLAN.

Beginning with software release E.08.xx, the switch allows up to 400 802.1p priority rules and/or DSCP policies in any combination. For more information, refer to “Maximum QoS Configuration Entries” under “QoS Operating Notes” on page 8-58.

You can configure a QoS priority of 0 through 7 for an outbound packet. When the packet is then sent to a port, the QoS priority determines which outbound queue the packet uses:

**Table 8-1. QoS Priority Settings and Operation**

<table>
<thead>
<tr>
<th>QoS Priority Setting</th>
<th>Outbound Port Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 2</td>
<td>low priority</td>
</tr>
<tr>
<td>0 - 3</td>
<td>normal priority</td>
</tr>
<tr>
<td>4 - 5</td>
<td>medium priority</td>
</tr>
<tr>
<td>6 - 7</td>
<td>high priority</td>
</tr>
</tbody>
</table>

If a packet is not in an 802.1Q tagged VLAN environment, then the QoS settings in table 8-1 control only to which outbound queue the packet goes. No priority is added to the packet for downstream device use. But if the packet is in an 802.1Q tagged VLAN environment, then the above setting is also added to the packet as an 802.1p priority for use by downstream devices and applications. (Shown in the next table. In either case, an IP packet can also carry a priority policy to downstream devices by using codepoint-marking in the ToS byte.)

**Table 8-1. Mapping Series 5300XL QoS Priority Settings to Device Queues**

<table>
<thead>
<tr>
<th>Priority Setting in the 5300XL Switches</th>
<th>Outbound Port Queues in the 5300XL Switches</th>
<th>802.1p Priority Setting Added to Tagged VLAN Packets Leaving the Switch</th>
<th>Queue Assignment in Downstream Devices With:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1 (low priority)</td>
<td>8 Queues</td>
</tr>
<tr>
<td></td>
<td>Queue 1</td>
<td>2</td>
<td>3 Queues</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0 (normal priority)</td>
<td>2 Queues</td>
</tr>
<tr>
<td></td>
<td>Queue 2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>4 (medium priority)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Queue 3</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>6 (high priority)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Queue 4</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>

8-7
Classifiers for Prioritizing Outbound Packets

You can configure QoS prioritization on the basis of seven QoS classifiers, or packet criteria, evaluated in the following order:

<table>
<thead>
<tr>
<th>Precedence</th>
<th>QoS Classifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UDP/TCP Application Type (port)</td>
</tr>
<tr>
<td>2</td>
<td>Device Priority (destination or source IP address)</td>
</tr>
<tr>
<td>3</td>
<td>IP Type of Service (ToS) field (IP packets only)</td>
</tr>
<tr>
<td>4</td>
<td>Protocol Priority (IP, IPX, ARP, DEC LAT, AppleTalk, SNA, and NetBeui)</td>
</tr>
<tr>
<td>5</td>
<td>VLAN Priority</td>
</tr>
<tr>
<td>6</td>
<td>Incoming source-port on the switch</td>
</tr>
<tr>
<td>7</td>
<td>Incoming 802.1p Priority (present in tagged VLAN environments)</td>
</tr>
</tbody>
</table>

If the switch is configured with multiple classifiers that address the same packet, the switch uses only the QoS configuration for the QoS classifier that has the highest precedence. (In this case, the QoS configuration for another, lower-precedence classifier that may apply is ignored.) For example, if QoS assigns high priority to “red” VLAN packets, but normal priority to IP packets, since Protocol Priority (4) has precedence over VLAN priority (5), IP packets on the “red” VLAN will be set to normal priority. See Table 8-2. "Precedence Criteria for QoS Classifiers" on page 8-9 for more information.

**Note On Using Multiple Criteria**

HP recommends that you configure a minimum number of the available QoS classifiers for prioritizing any given packet type. Increasing the number of active classifier options for a packet type increases the complexity of the possible outcomes.
### Table 8-2. Precedence Criteria for QoS Classifiers

<table>
<thead>
<tr>
<th>Precedence</th>
<th>Criteria</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>UDP/TCP</td>
<td>Takes precedence based on a layer 4 UDP or TCP application, with a user-specified application port number (for example, Telnet). <strong>Default state:</strong> Disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a packet does not meet the criteria for UDP/TCP priority, then precedence defaults to the Device Priority classifier, below.</td>
</tr>
<tr>
<td>2</td>
<td>Device Priority (IP Address)</td>
<td>Takes precedence based on an outbound packet having a particular destination or source IP address. QoS allows up to 256 IP addresses. If an outbound packet has an IP address as the destination, it takes precedence over another outbound packet that has the same IP address as a source. (This can occur, for example, on an outbound port in a switch mesh environment.) Also, if the source and destination IP addresses (SA and DA) in the same packet match, the DA takes precedence. <strong>Default state:</strong> No IP address prioritization.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a packet does not meet the criteria for device priority, then precedence defaults to the IP Type of Service (ToS) classifier, below.</td>
</tr>
<tr>
<td>3</td>
<td>IP Type-of-Service (ToS)</td>
<td>Takes precedence based on the TOS field in IP packets. (Applies only to IP packets.) The ToS field is configured by an upstream device or application before the packet enters the switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>IP Precedence Mode:</strong> QoS reads the packet’s IP precedence (upper three) bits in the Type-of-Service (ToS) byte and automatically prioritizes the packet (if specified in the QoS configuration) for outbound transmission.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Differentiated Services Mode:</strong> QoS reads the packet’s differentiated services, or codepoint (upper six) bits of the Type-of-Service (TOS) byte. Packet prioritization depends on the configured priority for the codepoint. (Some codepoints default to the DSCP standard, but can be overridden.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more on this topic, see “QoS IP Type-of-Service (ToS) Policy and Priority” on page 8-24.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Default state:</strong> Disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a packet does not meet the criteria for ToS priority, then precedence defaults to the Protocol classifier, below.</td>
</tr>
<tr>
<td>4</td>
<td>Layer 3 Protocol Priority</td>
<td>Takes precedence based on network protocols: IP, IPX, ARP, DEC LAT, AppleTalk, SNA, and NetBeui. <strong>Default state:</strong> No-override for any protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a packet does not meet the criteria for Protocol priority, then precedence defaults to the VLAN classifier, below.</td>
</tr>
<tr>
<td>5</td>
<td>VLAN Priority</td>
<td>Takes precedence based on the ID number of the VLAN in which the packet exists. For example, if the default VLAN (VID = 1) and the “Blue” VLAN (with a VID of 20) are both assigned to a port, and Blue VLAN traffic is more important, you can configure QoS to give Blue VLAN traffic a higher priority than default VLAN traffic. (Priority is applied on the outbound port.) <strong>Default state:</strong> No-override.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a packet does not meet the criteria for VLAN priority, then precedence defaults to the Source-Port classifier, below.</td>
</tr>
</tbody>
</table>
Quality of Service (QoS): Managing Bandwidth More Effectively

Introduction

<table>
<thead>
<tr>
<th>Precedence</th>
<th>Criteria</th>
<th>Overview</th>
</tr>
</thead>
</table>
| 6-         | Source-Port | Takes precedence based on the source-port (that is, the port on which the packet entered the switch).
|            |          | If a packet does not meet the criteria for source-port priority, then precedence defaults to Incoming 802.1p criteria, below |

| 7-         | Incoming 802.1p Priority | Where a packet enters the switch on a tagged VLAN, if QoS is not configured to override the packet's priority setting, the switch uses the packet's existing 802.1p priority (assigned by an upstream device or application) to determine which inbound and outbound port queue to use. If the packet leaves the switch on a tagged VLAN, then there is no change to its 802.1p priority setting. If the packet leaves the switch on an untagged VLAN, the 802.1p priority is dropped. |

<table>
<thead>
<tr>
<th>Entering (Inbound) 802.1p Priority</th>
<th>Outbound Port Queue</th>
<th>Exiting (Outbound) 802.1p Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 2</td>
<td>Low</td>
<td>1 - 2</td>
</tr>
<tr>
<td>0 - 3</td>
<td>Normal</td>
<td>0 - 3</td>
</tr>
<tr>
<td>4 - 5</td>
<td>Medium</td>
<td>4 - 5</td>
</tr>
<tr>
<td>6 - 7</td>
<td>High</td>
<td>6 - 7</td>
</tr>
</tbody>
</table>

If a packet does not meet the criteria for Incoming 802.1p priority, then the packet goes to the “normal” outbound queue of the appropriate port. If the packet entered the switch on an untagged VLAN, but exits on a tagged VLAN, then a tagged VLAN field, including an 802.1p priority of 0 (normal), is added to the packet.

No Override. By default, the IP ToS, Protocol, and VLAN-ID criteria automatically list each of their priority options as No-override. (Some IP TOs codepoints use default priority settings defined by the DSCP standard.) This means that if you do not configure a priority for a specific option, QoS does not prioritize packets to which that option applies. For example, if you do not specify a priority for the IP protocol, then the IP protocol will not be a criteria for setting a QoS priority and the packets will be handled as described above.
Preparation for Configuring QoS

You can use QoS regardless of whether your network has tagged VLANs:

Table 8-3. Summary of QoS Capabilities

<table>
<thead>
<tr>
<th>Outbound Packet Options</th>
<th>Tagged VLAN Environment</th>
<th>No Tagged VLANs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Queue Priority for Packet Types</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Carry the 802.1p Priority Assignment to Next Downstream Device</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Configure a Service Policy and Carry It to Downstream Devices.</td>
<td>Yes ¹</td>
<td>Yes ¹</td>
</tr>
</tbody>
</table>

The policy includes:
- Assigning a ToS Codepoint
- Assigning an 802.1p Priority ² to the Codepoint

¹ Except for packets processed using either the (Layer 3) Protocol or QoS IP-Precedence methods. Also, to use a service policy in this manner, the downstream devices must be configured to interpret and use the DSCP carried in the IP packets.

² This priority corresponds to the 802.1p priority scheme and is used to determine the packet's port queue priority. When used in a tagged VLAN environment, this priority is also assigned as the 802.1p priority carried outbound in tagged VLAN packets.

Steps for Configuring QoS on the Switch

1. Determine the QoS policy you want to implement. This includes analyzing the types of traffic flowing through your network and identifying one or more traffic types to prioritize. In order of precedence, these are:
   a. UDP/TCP applications
   b. Device Priority—destination or source IP address (Note that destination has precedence over source. See Table 8-2.)
   c. IP Type-of-Service Precedence Bits (Leftmost three bits in the ToS field of IP packets)
   d. IP Type-of-Service Differentiated Service bits (Leftmost six bits in the ToS field of IP packets)
   e. Protocol Priority
   f. VLAN Priority (requires at least one tagged VLAN on the network)
   g. Source-Port
   h. Incoming 802.1p Priority (requires at least one tagged VLAN on the network)

   For more on how QoS operates with the above traffic types, see Table 8-2. "Precedence Criteria for QoS Classifiers" on page 8-9.)
2. Select the QoS option you want to use. Table 8-4 lists the traffic types (QoS classifiers) and the QoS options you can use for prioritizing or setting a policy on these traffic types:

### Table 8-4. Applying QoS Options to Traffic Types Defined by QoS Classifiers

<table>
<thead>
<tr>
<th>QoS Options for Prioritizing Outbound Traffic</th>
<th>QoS Classifiers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UDP/TCP</td>
</tr>
<tr>
<td><strong>Option 1: Set 802.1p Priority Only</strong></td>
<td></td>
</tr>
<tr>
<td>Prioritize traffic by sending specific packet types (determined by QoS classifier) to different outbound port queues on the switch. Rely on tagged VLANs to carry packet priority as an 802.1p value to downstream devices.</td>
<td></td>
</tr>
<tr>
<td><strong>Option 2: Configure ToS DSCP Policy with 802.1p Priority</strong></td>
<td></td>
</tr>
<tr>
<td>Prioritize traffic by sending specific packet types (determined by QoS classifier) to different outbound port queues on the switch. Propagate a service policy by reconfiguring the DSCP in outbound IP packets according to packet type. (Assumes that downstream devices can be configured to recognize the DSCP in IP packets and implement the service policy it indicates.) Use tagged VLANs to carry packet priority as an 802.1p value to downstream devices.</td>
<td></td>
</tr>
</tbody>
</table>

1. In this mode the configuration is fixed. You cannot change the automatic priority assignment when using IP-ToS Precedence as a QoS classifier.

3. If you want 802.1p priority settings to be included in outbound packets, ensure that tagged VLANs are configured on the appropriate links.

4. Determine the actual QoS configuration changes you will need to make on each QoS-capable device in your network in order to implement the desired policy. Also, if you want downstream devices to read and use DSCPs in IP packets from the switch, configure them to do so by enabling ToS Differentiated Service mode and making sure the same DSCP policies are configured.
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

<table>
<thead>
<tr>
<th>QoS Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP/TCP Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 8-13</td>
<td>page 8-56</td>
</tr>
<tr>
<td>IP-Device Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 8-19</td>
<td>&quot;</td>
</tr>
<tr>
<td>IP Type-of-Service Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 8-24</td>
<td>&quot;</td>
</tr>
<tr>
<td>LAN Protocol Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 8-36</td>
<td>&quot;</td>
</tr>
<tr>
<td>VLAN-ID Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 8-38</td>
<td>&quot;</td>
</tr>
<tr>
<td>Source-Port Priority</td>
<td>Disabled</td>
<td>—</td>
<td>page 8-43</td>
<td>&quot;</td>
</tr>
</tbody>
</table>

QoS UDP/TCP Priority

QoS Classifier Precedence: 1

When you use UDP or TCP and a layer 4 Application port number as a QoS classifier, traffic carrying the specified UDP/TCP port number(s) is marked with the UDP/TCP classifier's configured priority level, without regard for any other QoS classifiers in the switch.

Options for Assigning Priority. Priority control options for TCP or UDP packets carrying a specified TCP or UDP port number include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an associated 802.1p priority; inbound packets must be IPv4.)

For a given TCP or UDP port number, you can use only one of the above options at a time. However, for different port numbers, you can use different options.

TCP/UDP Port Number Ranges. There are three ranges:

- Well-Known Ports: 0 - 1023
- Registered Ports: 1024 - 49151
- Dynamic and/or Private Ports: 49152 - 65535

For more information, including a listing of UDP/TCP port numbers, go to the Internet Assigned Numbers Authority (IANA) website at:

http://www.iana.org
Then click on:

**Protocol Number Assignment Services**

P (Under “Directory of General Assigned Numbers” heading)

**Port Numbers**

Assigning a Priority Based on TCP or UDP Port Number

This option assigns an 802.1p priority to outbound TCP or UDP packets as described below.

**Syntax:**

```
qos < udp-port | tcp-port > < tcp or udp port number > priority < 0 - 7 >
```

Configures an 802.1p priority for outbound packets having the specified TCP or UDP application port number. This priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device.

(Default: Disabled)

```
no qos < udp-port | tcp-port > < tcp-udp port number >
```

Deletes the specified UDP or TCP port number as a QoS classifier.

```
show qos tcp-udp-port-priority
```

Displays a listing of all TCP and UDP QoS classifiers currently in the running-config file.

For example, configure and list 802.1p priority for the following UDP and TCP port prioritization:

<table>
<thead>
<tr>
<th>TCP/UDP Port</th>
<th>802.1p Priority for TCP</th>
<th>802.1p Priority for UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Port 23 (Telnet)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>UDP Port 23 (Telnet)</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>TCP Port 80 (World Wide Web HTTP)</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>UDP Port 80 (World Wide Web HTTP)</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Assigning a DSCP Policy Based on TCP or UDP Port Number

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound TCP or UDP packets having the specified port number. That is, the switch:

1. Selects an incoming IP packet if the TCP or UDP port number it carries matches the port number specified in the TCP or UDP classifier (as shown in figure 8-3, above).

2. Overwrites the packet’s DSCP with the DSCP configured in the switch for such packets.

3. Assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)

4. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, refer to “Terminology” on page 8-5.
Steps for Creating a DSCP Policy Based on TCP/UDP Port Number Classifiers. This procedure creates a DSCP policy for IP packets carrying the selected UDP or TCP port-number classifier.

1. Identify the TCP or UDP port-number classifier you want to use for assigning a DSCP policy.

2. Determine the DSCP policy for packets carrying the selected TCP or UDP port number.
   a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite the DSCP carried in packets received from upstream devices.)
   b. Determine the 802.1p priority you want to assign to the DSCP.

3. Configure the DSCP policy by using `qos dscp-map` to configure the priority to the codepoint you selected in step 2a. (For details, refer to the example later in this section, and to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)

**Note**

A codepoint must have an 802.1p priority assignment (0 - 7) before you can configure a policy for prioritizing packets by TCP or UDP port numbers. If a codepoint you want to use shows **No-override** in the Priority column of the DSCP map (show qos dscp-map), then you must assign a 0 - 7 priority before proceeding.

4. Configure the switch to assign the DSCP policy to packets with the specified TCP or UDP port number.

**Syntax:** `qos dscp-map < codepoint > priority < 0 - 7 >`

This command is optional if a priority has already been assigned to the `<codepoint>`. The command creates a DSCP policy by assigning an 802.1p priority to a specific DSCP. When the switch applies this policy to a packet, the priority determines the packet’s queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. If the packet is IPv4, the packet’s DSCP will be replaced by the codepoint specified in this command. (Default: For most codepoints, **No-override**. See figure 8-8-6 on page 8-51.)
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

Syntax: qos < udp-port | tcp-port > < tcp or udp port number > dscp < codepoint >

Assigns a DSCP policy to packets having the specified TCP or UDP application port number and overwrites the DSCP in these packets with the assigned <codepoint> value. This policy includes an 802.1p priority and determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. (Default: No-override)

no qos < udp-port | tcp-port > < tcp-udp port number >

Deletes the specified UDP or TCP port number as a QoS classifier.

show qos tcp-udp-port-priority

Displays a listing of all TCP and UDP QoS classifiers currently in the running-config file.

For example, suppose you wanted to assign these DSCP policies to the packets identified by the indicated UDP and TDP port applications:

<table>
<thead>
<tr>
<th>Port Applications</th>
<th>DSCP Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DSCP</td>
</tr>
<tr>
<td>23-UDP</td>
<td>000111</td>
</tr>
<tr>
<td>80-TDP</td>
<td>000101</td>
</tr>
<tr>
<td>914-TDP</td>
<td>000010</td>
</tr>
<tr>
<td>1001-UDP</td>
<td>000010</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. (Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

Figure 8-4. Display the Current DSCP-Map Configuration
2. Configure the DSCP policies for the codepoints you want to use.

```
HPswitch(config)# qos dscp-map 000111 priority 7
HPswitch(config)# qos dscp-map 000101 priority 5
HPswitch(config)# qos dscp-map 000010 priority 1
HPswitch(config)# show qos dscp-map

DSCP -> 802.1p priority mappings
DSCP policy 802.1p tag Policy name
----------------- ------------- --------------
000000  No-override
000001  No-override 000010  1
000011  No-override
000100  No-override 000101  5
000110  No-override
000111  7
001000  No-override

Figure 8-5. Assign Priorities to the Selected DSCPs
```

3. Assign the DSCP policies to the selected UDP/TCP port applications and display the result.

```
HPswitch(config)# qos udp-port 23 dscp 000111
HPswitch(config)# qos tcp-port 80 dscp 000101
HPswitch(config)# qos tcp-port 914 dscp 000010
HPswitch(config)# qos udp-port 1001 dscp 000010
HPswitch(config)# show qos tcp-udp-port-priority

TCP/UDP port based priorities

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Application</th>
<th>Port</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td></td>
<td>23</td>
<td>DSCP</td>
<td>000111</td>
<td>7</td>
</tr>
<tr>
<td>TCP</td>
<td></td>
<td>80</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>TCP</td>
<td></td>
<td>914</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>UDP</td>
<td></td>
<td>1001</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
</tbody>
</table>
```

```
Figure 8-6. The Completed DSCP Policy Configuration for the Specified UDP/TCP Port Applications
```

The switch will now apply the DSCP policies in figure 8-6 to IP packets received in the switch with the specified UDP/TCP port applications. This means the switch will:

- Overwrite the original DSCPs in the selected packets with the new DSCPs specified in the above policies.
- Assign the 802.1p priorities in the above policies to the selected packets.
QoS IP-Device Priority

QoS Classifier Precedence: 2

The IP device option enables you to use up to 256 IP addresses (source or destination) as QoS classifiers. Where a particular device-IP address classifier has the highest precedence in the switch for traffic addressed to or from that device, then traffic received on the switch with that address is marked with the IP address classifier's configured priority level. Different IP device classifiers can have differing priority levels.

Options for Assigning Priority. Priority control options for packets carrying a specified IP address include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an 802.1p priority; inbound packets must be IPv4.)

(For operation when other QoS classifiers apply to the same traffic, refer to “Classifiers for Prioritizing Outbound Packets” on page 8-8.)

For a given IP address, you can use only one of the above options at a time. However, for different IP addresses, you can use different options.

Assigning a Priority Based on IP Address

This option assigns an 802.1p priority to all outbound packets having the specified IP address as either a source or destination. (If both match, the priority for the IP destination address has precedence.)

Syntax:  qos device-priority < ip-address > priority < 0 - 7 >

Configures an 802.1p priority for outbound packets having the specified IP address. This priority determines the packet’s queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. (Default: Disabled)

no qos device-priority < ip-address >

Removes the specified IP device-priority QoS classifier and resets the priority for that VLAN to No-override.

show qos device-priority

Displays a listing of all IP device-priority QoS classifiers currently in the running-config file.
For example, configure and list the 802.1p priority for packets carrying the following IP addresses:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>802.1p Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.28.31.1</td>
<td>7</td>
</tr>
<tr>
<td>10.28.31.130</td>
<td>5</td>
</tr>
<tr>
<td>10.28.31.100</td>
<td>1</td>
</tr>
<tr>
<td>10.28.31.101</td>
<td>1</td>
</tr>
</tbody>
</table>

```
HPswitch(config)# qos device-priority 10.28.31.1 priority 7
HPswitch(config)# qos device-priority 10.28.31.130 priority 5
HPswitch(config)# qos device-priority 10.28.31.100 priority 1
HPswitch(config)# qos device-priority 10.28.31.101 priority 1
```

```
HPswitch(config)# show qos device-priority
Device priorities
Device Address  Apply rule | DSCP | Priority
---------------|-------|--------|
10.28.31.1      Priority | 7     |
10.28.31.130    Priority | 5     |
10.28.31.100    Priority | 1     |
10.28.31.101    Priority | 1     |
```

Figure 8-7. Example of Configuring and Listing 802.1p Priority Assignments for Packets Carrying Specific IP Addresses

Assigning a DSCP Policy Based on IP Address

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets having the specified IP address (either source or destination). That is, the switch:

1. Selects an incoming IP packet on the basis of the source or destination IP address it carries.
2. Overwrites the packet’s DSCP with the DSCP configured in the switch for such packets, and assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)
3. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, refer to “Terminology” on page 8-5.

**Steps for Creating a Policy Based on IP Address.** This procedure creates a DSCP policy for IP packets carrying the selected IP address (source or destination).
1. Identify the IP address you want to use as a classifier for assigning a DSCP policy.

2. Determine the DSCP policy for packets carrying the selected IP address:
   a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite the DSCP carried in packets received from upstream devices.)
   b. Determine the 802.1p priority you want to assign to the DSCP.

3. Configure the DSCP policy by using `dscp-map` to configure the priority to the codepoint you selected in step 2a. (For details, refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)

   **Note**

   A codepoint must have an 802.1p priority assignment (0 - 7) before you can configure a policy for prioritizing packets by IP address. If a codepoint you want to use shows **No-override** in the **Priority** column of the DSCP map (show qos dscp-map), then you must assign a 0 - 7 priority before proceeding.

4. Configure the switch to assign the DSCP policy to packets with the specified IP address.

   **Syntax:** `qos dscp-map < codepoint > priority < 0 - 7 >`

   *This command is optional if a priority has already been assigned to the < codepoint >. The command creates a DSCP policy by assigning an 802.1p priority to a specific DSCP. When the switch applies this policy to a packet, the priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. If the packet is IPv4, the packet's DSCP will be replaced by the codepoint specified in this command. (Default: For most codepoints, No-override. See figure 8-8-6 on page 8-51.)*

   **Syntax:** `qos device-priority < ip-address > dscp < codepoint >`

   *Assigns a DSCP policy to packets carrying the specified IP address, and overwrites the DSCP in these packets with the assigned < codepoint > value. This policy includes an 802.1p priority and determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. (Default: No-override)*
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

no qos device-priority < ip-address >

Deletes the specified IP address as a QoS classifier.

show qos device-priority

Displays a listing of all QoS Device Priority classifiers currently in the running-config file.

For example, suppose you wanted to assign these DSCP policies to the packets identified by the indicated IP addresses:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>DSCP Policies</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.28.31.1</td>
<td>000111</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>10.28.31.130</td>
<td>000101</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>10.28.31.100</td>
<td>000010</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>10.28.31.101</td>
<td>000010</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP. (Refer to the “Note On Changing a Priority Setting” on page 8-53. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

<table>
<thead>
<tr>
<th>HPswitch(config)# show qos dscp-map</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>DSCP policy</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>000000</td>
</tr>
<tr>
<td>000001</td>
</tr>
<tr>
<td>000010</td>
</tr>
<tr>
<td>000011</td>
</tr>
<tr>
<td>000100</td>
</tr>
<tr>
<td>000101</td>
</tr>
<tr>
<td>000110</td>
</tr>
<tr>
<td>000111</td>
</tr>
</tbody>
</table>

Figure 8-8. Display the Current DSCP-Map Configuration
2. Configure the priorities for the DSCPs you want to use.

```plaintext
HPswitch(config)# qos dscp-map 000111 priority 7
HPswitch(config)# qos dscp-map 000101 priority 5
HPswitch(config)# qos dscp-map 000010 priority 1
HPswitch(config)# show qos dscp-map
   DSCP -> 802.1p priority mappings
   DSCP policy 802.1p tag   Policy name
   -----------------------------------------------
   000000   No-override
   000001   No-override
   000010   1                      DSCP Policies Configured in this step.
   000011   No-override
   000100   No-override
   000101   5
   000110   No-override
   000111   7
   001000   No-override
   ...
```

**Figure 8-9. Assigning 802.1p Priorities to the Selected DSCPs**

3. Assign the DSCP policies to the selected device IP addresses and display the result.

```plaintext
HPswitch(config)# qos device-priority 10.28.31.1 dscp 000111
HPswitch(config)# qos device-priority 10.28.31.130 dscp 000101
HPswitch(config)# qos device-priority 10.28.31.100 dscp 000010
HPswitch(config)# qos device-priority 10.28.31.101 dscp 000010
HPswitch(config)# show qos device-priority
   Device priorities
   Device Address        Apply rule  DSCP  Priority
   ---------------------  ------------  ----  ----
   10.28.31.1            DSCP        000111  7
   10.28.31.130           DSCP       000101  5
   10.28.31.100           DSCP       000010  1
   10.28.31.101           DSCP       000010  1
```

**Figure 8-10. The Completed Device-Priority/Codepoint Configuration**

The switch will now apply the DSCP policies in figure 8-9 to packets received on the switch with the specified IP addresses (source or destination). This means the switch will:

- Overwrite the original DSCPs in the selected packets with the new DSCPs specified in the above policies.
- Assign the 802.1p priorities in the above policies to the appropriate packets.
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

QoS IP Type-of-Service (ToS) Policy and Priority

QoS Classifier Precedence: 3

This feature applies only to IP traffic and performs either of the following:

- **ToS IP-Precedence Mode**: All IP packets generated by upstream devices and applications include precedence bits in the ToS byte. Using this mode, the switch uses these bits to compute and assign the corresponding 802.1p priority.

- **ToS Differentiated Services (Diffserv) Mode**: This mode requires knowledge of the codepoints set in IP packets by the upstream devices and applications. It uses the ToS codepoint in IP packets coming from upstream devices and applications to assign 802.1p priorities to the packets. You can use this option to do both of the following:
  - **Assign a New Prioritization Policy**: A “policy” includes both a codepoint and a corresponding 802.1p priority. This option selects an incoming IP packet on the basis of its codepoint and assigns a new codepoint and corresponding 802.1p priority. (Use the `qos dscp-map` command to specify a priority for any codepoint—page 8-50.)
  - **Assign an 802.1p Priority**: This option reads the DSCP of an incoming IP packet and, without changing this codepoint, assigns the 802.1p priority to the packet, as configured in the DSCP Policy Table (page 8-50). This means that a priority value of 0 - 7 must be configured for a DSCP before the switch will attempt to perform a QoS match on the packet’s DSCP bits.

Before configuring the ToS Diffserv mode, you must use the `dscp-map` command to configure the desired 802.1p priorities for the codepoints you want to use for either option. This command is illustrated in the following examples and is described under “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.

Unless IP-Precedence mode and Diffserv mode are both disabled (the default setting), enabling one automatically disables the other. For more on ToS operation, refer to “Details of QoS IP Type-of-Service” on page 8-33.
Assigning an 802.1p Priority to IP Packets on the Basis of the ToS Precedence Bits

If a device or application upstream of the switch sets the precedence bits in the ToS byte of IP packets, you can use this feature to apply that setting for prioritizing packets for outbound port queues. If the outbound packets are in a tagged VLAN, this priority is carried as an 802.1p value to the adjacent downstream devices.

**IP Precedence Syntax:** `qos type-of-service ip-precedence`

*Causes the switch to automatically assign an 802.1p priority to all IP packets by computing each packet's 802.1p priority from the precedence bits the packet carries. This priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. (ToS IP Precedence Default: Disabled)*

**no qos type-of-service**

*Disables all ToS classifier operation, including prioritization using the precedence bits.*

**show qos type-of-service**

*When ip-precedence is enabled (or if neither ToS option is configured), shows the ToS configuration status. If diff-services is enabled, lists codepoint data as described under “Assigning a DSCP Policy on the Basis of the DSCP in IP Packets Received from Upstream Devices” on page 8-30.*

With this option, prioritization of outbound packets relies on the IP-Precedence bit setting that IP packets carry with them from upstream devices and applications. To configure and verify this option:

```
HPswitch(config)# qos type-of-service ip-precedence
HPswitch(config)# show qos type-of-service
  Type of Service [Disabled] : IP Precedence

Figure 8-11. Example of Enabling ToS IP-Precedence Prioritization
```
To replace this option with the ToS diff-services option, just configure **diff services** as described below, which automatically disables IP-Precedence. To disable IP-Precedence without enabling the diff-services option, use this command:

```
HPswitch(config)# no qos type-of-service
```

**Assigning an 802.1p Priority to IP Packets on the Basis of Incoming DSCP**

One of the best uses for this option is on an interior switch where you want to honor (continue) a policy set on an edge switch. That is, it enables you to select incoming packets having a specific DSCP and forward these packets with the desired 802.1p priority. For example, if an edge switch “A” marks all packets received on port A5 with a particular DSCP, you can configure a downstream (interior) switch “B” to handle such packets with the desired priority (regardless of whether 802.1Q tagged VLANs are in use).

![Figure 8-12. Interior Switch “B” Honors the Policy Established in Edge Switch “A”](image)

To do so, assign the desired 802.1p priority to the same codepoint that the upstream or edge switch assigns to the selected packets. When the downstream switch receives an IP packet carrying one of these codepoints, it assigns the configured priority to the packet and sends it out the appropriate priority queue. (The packet retains the codepoint it received from the upstream or edge switch). You can use this option concurrently with the diffserv DSCP Policy option (described later in this section), as long as the DSCPs specified in the two options do not match.
Operating Notes

Different applications may use the same DSCP in their IP packets. Also, the same application may use multiple DCSPs if the application originates on different clients, servers, or other devices. Using an edge switch enables you to select the packets you want and mark them with predictable DCSPs that can be used by downstream switches to honor policies set in the edge switch.

When enabled, the switch applies direct 802.1p prioritization to all packets having codepoints that meet these criteria:

- The codepoint is configured with an 802.1p priority in the DCSP table.
  (Codepoints configured with No-override are not used.)
- The codepoint is not configured for a new DCSP policy assignment.

Thus, the switch does not allow the same incoming codepoint (DCSP) to be used simultaneously for directly assigning an 802.1p priority and also assigning a DCSP policy. For a given incoming codepoint, if you configure one option and then the other, the second overwrites the first.

To use this option:

1. Identify a DCSP used to set a policy in packets received from an upstream or edge switch.

2. Determine the 802.1p priority (0 - 7) you want to apply to packets carrying the identified DCSP. (You can either maintain the priority assigned in the upstream or edge switch, or assign a new priority.)

3. Use `qos dscp-map < codepoint > priority < 0 - 7 >` to assign the 802.1p priority you want to the specified DCSP. (For more on this topic, refer to “Differentiated Services Codepoint (DCSP) Mapping” on page 8-50.)

4. Enable `diff-services`
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic


Syntax: qos type-of-service diff-services

Causes the switch to read the DSCP of an incoming IP packet and, when a match occurs, assign a corresponding 802.1p priority, as configured in the switch’s DSCP table (page 8-51).

no qos type-of-service

Disables all ToS classifier operation.

no qos dscp-map < codepoint>

Disables direct 802.1p priority assignment to packets carrying the < codepoint > by reconfiguring the codepoint priority assignment in the DSCP table to No-override. Note that if this codepoint is in use as a DSCP policy for another diffserv codepoint, you must disable or redirect the other diffserv codepoint’s DSCP policy before you can disable or change the codepoint. For example, in figure 8-13 you cannot change the priority for the 000000 codepoint until you redirect the DSCP policy for 000001 away from using 000000 as a policy. (Refer to “Note On Changing a Priority Setting” on page 8-53. Refer also to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)

show qos type-of-service

Displays current Type-of-Service configuration. In diffserv mode it also shows the current direct 802.1p assignments and the current DSCP assignments covered later in this section.

For example, an edge switch “A” in an untagged VLAN assigns a DSCP of 000110 on IP packets it receives on port A6, and handles the packets with high priority (7). When these packets reach interior switch “B” you want the switch to handle them with the same high priority. To enable this operation you would
configure an 802.1p priority of 7 for packets received with a DSCP of 000110, and then enable **diff-services**:

```
HPswitch(config)# show qos type-of-service
Type of Service [Disabled] : Disabled

<table>
<thead>
<tr>
<th>Codepoint</th>
<th>DSCP Policy</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>000000</td>
<td>1</td>
</tr>
<tr>
<td>000001</td>
<td>000000</td>
<td>1</td>
</tr>
<tr>
<td>000010</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>000111</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>001000</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>001001</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>001010</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>001111</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Executing this command displays the current ToS configuration and shows that the selected DSCP is not currently in use.

The 000110 codepoint is unused, and thus available for directly assigning an 802.1p priority without changing the packet’s DSCP.

**Note:** All codepoints without a “DSCP Policy” entry are available for direct 802.1p priority assignment.

**Figure 8-13. Example Showing Codepoints Available for Direct 802.1p Priority Assignments**

```
HPswitch(config)# qos dscp-map 000110 priority 7
HPswitch(config)# qos type-of-service diff-services
```

```
Type of Service [Disabled] : Differentiated Services

<table>
<thead>
<tr>
<th>Codepoint</th>
<th>DSCP Policy</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>000000</td>
<td>1</td>
</tr>
<tr>
<td>000001</td>
<td>000000</td>
<td>1</td>
</tr>
<tr>
<td>000010</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>000111</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>001000</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>001001</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>001010</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>001111</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Outbound IP packets with a DSCP of 000110 will have a priority of 7.

Notice that codepoints 000000 and 001001 are named as DSCP policies by other codepoints (000001 and 000110 respectively). This means they are not available for changing to a different 802.1p priority.

**Figure 8-14. Example of a Type-of-Service Configuration Enabling Both Direct 802.1p Priority Assignment and DSCP Policy Assignment**
Assigning a DSCP Policy on the Basis of the DSCP in IP Packets Received from Upstream Devices

The preceding section describes how to forward a policy set by an edge (or upstream) switch. This option changes a DSCP policy in an outbound IP packet by changing its IP ToS codepoint and applying the priority associated with the new codepoint. (A DSCP policy consists of a differentiated services codepoint and an associated 802.1p priority.) You can use this option concurrently with the diffserv 802.1p priority option (above), as long as the DSCPs specified in the two options do not match.

To use this option to configure a change in policy:

1. Identify a DSCP used to set a policy in packets received from an upstream or edge switch.

2. Create a new policy by using `qos dscp-map < codepoint > priority < 0 - 7 >` to configure an 802.1p priority for the codepoint you will use to overwrite the DSCP the packet carries from upstream. (For more on this topic, refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)

3. Use `qos type-of-service diff-services < incoming-DSCP > dscp < outgoing-DSCP >` to change the policy on packets coming from the edge or upstream switch with the specified incoming DSCP.

(Figure 8-12 on page 8-26 illustrates this scenario.)

**Syntax:** `qos type-of-service diff-services`

**Enables ToS diff-services.**

```
qos type-of-service diff-services < current-codepoint > dscp < new-codepoint >
```

Configures the switch to select an incoming IP packet carrying the `<current-codepoint>` and then use the `<new-codepoint>` to assign a new, previously configured DSCP policy to the packet. The policy overwrites the `<current-codepoint>` with the `<new-codepoint>` and assigns the 802.1p priority specified by the policy. (Use the `qos dscp-map` command to define the priority for the DSCPs—page 8-50.)

```
no qos type-of-service
```

Disables all ToS classifier operation. Current ToS DSCP policies and priorities remain in the configuration and will become available if you re-enable ToS diff-services.
no qos type-of-service [diff-services < codepoint>]

Deletes the DSCP policy assigned to the <codepoint> and returns the <codepoint> to the 802.1p priority setting it had before the DSCP policy was assigned. (This will be either a value from 0 - 7 or No-override.)

show qos type-of-service

Displays a listing of codepoints, with any corresponding DSCP policy re-assignments for outbound packets. Also lists the (802.1p) priority for each codepoint that does not have a DSCP policy assigned to it.

For example, suppose you want to configure the following two DSCP policies for packets received with the indicated DSCPs.

<table>
<thead>
<tr>
<th>Received DSCP</th>
<th>Policy DSCP</th>
<th>802.1p Priority</th>
<th>Policy Name (Optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td>001100</td>
<td>000010</td>
<td>6</td>
<td>Level 6</td>
</tr>
<tr>
<td>001101</td>
<td>000101</td>
<td>4</td>
<td>Level 4</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP. (Refer to the “Note On Changing a Priority Setting” on page 8-53. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

The DSCPs for this example have not yet been assigned an 802.1p priority level.

Figure 8-15. Display the Current DSCP-Map Configuration
2. Configure the policies in the DSCP table:

```
HPswitch(config)# qos dscp-map 000010 priority 6 name 'Level 6'
HPswitch(config)# qos dscp-map 000101 priority 4 name 'Level 4'
```

```
HPswitch(config)# show qos dscp-map
DSCP  802.1p priority mappings
DSCP policy 802.1p tag Policy name
---------- --------- -----------------------------------------------
 000000     No-override
 000001     No-override
 000010     6 Level 6
 000011     No-override
 000100     No-override
 000101     4 Level 4
 000110     No-override
 000111     No-override
 000110     
 000111     
```

**Figure 8-16. Example of Policies Configured (with Optional Names) in the DSCP Table**

3. Assign the policies to the codepoints in the selected packet types.

```
HPswitch(config)# qos type-of-service diff-services 001100 dscp 000010
HPswitch(config)# qos type-of-service diff-services 001101 dscp 000101
```

```
HPswitch(config)# show qos type-of-service
Type of Service [Disabled] : Differentiated Services
Codepoint DSCP Policy | Priority
---------- ------------|
 000000     No-override
 000001     No-override
 000010     6
 000011     No-override
 000100     No-override
 000101     4
 000110     No-override
 000111     No-override
 001000     No-override
 001001     1
 001010     
 001011     
 001100     
 001101     
 001110     
 001111     
 010000     
 010001     
```

**Figure 8-17. Example of Policy Assignment to Outbound Packets on the Basis of the DSCP in the Packets Received from Upstream Devices**
Details of QoS IP Type-of-Service

IP packets include a Type of Service (ToS) byte. The ToS byte includes:

- **A Differentiated Services Codepoint (DSCP):** This element is comprised of the upper six bits of the ToS byte). There are 64 possible codepoints. In the switch’s default qos configuration, some codepoints have default 802.1p priority settings for Assured-Forwarding and Expedited Forwarding, while others are unused (and listed with **No-override** for a Priority). Using the **qos dscp map** command, you can configure the switch to assign different prioritization policies to IP packets having different codepoints. As an alternative, you can configure the switch to assign a new codepoint to an IP packet, along with a corresponding 802.1p priority (0-7). To use this option in the simplest case, you would:
  a. Configure a specific DSCP with a specific priority in an edge switch.
  b. Configure the switch to mark a specific type of inbound traffic with that DSCP (and thus create a policy for that traffic type).
  c. Configure the internal switches in your LAN to honor the policy.

(For example, you could configure an edge switch to assign a codepoint of 000001 to all packets received from a specific VLAN, and then handle all traffic with that codepoint at high priority.)

For a codepoint listing and the commands for displaying and changing the DSCP Policy table, refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.

- **Precedence Bits:** This element is a subset of the DSCP and is comprised of the upper three bits of the ToS byte. When configured to do so, the switch uses the precedence bits to determine a priority for handling the associated packet. (The switch does not change the setting of the precedence bits.) Using the ToS Precedence bits to prioritize IP packets relies on priorities set in upstream devices and applications.
Figure 8-18 shows an example of the ToS byte in the header for an IP packet, and illustrates the diffserv bits and precedence bits in the ToS byte. (Note that the Precedence bits are a subset of the Differentiated Services bits.)

<table>
<thead>
<tr>
<th>Field:</th>
<th>Destination MAC Address</th>
<th>Source MAC Address</th>
<th>IP Identifier</th>
<th>Type &amp; Version</th>
<th>ToS Byte</th>
<th>...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet:</td>
<td>FF FF FF FF FF FF</td>
<td>08 00 00 00 16</td>
<td>08 00</td>
<td>45</td>
<td>E 0</td>
<td>...</td>
</tr>
</tbody>
</table>

**Figure 8-18. The ToS Codepoint and Precedence Bits**
## Quality of Service (QoS): Managing Bandwidth More Effectively
### Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

### Table 8-5. How the Switch Uses the ToS Configuration

<table>
<thead>
<tr>
<th>Outbound Port</th>
<th>ToS Option:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP Precedence (Value = 0 - 7)</td>
</tr>
<tr>
<td>IP Packet in an Un-tagged VLAN</td>
<td>Depending on the value of the IP Precedence bits in the packet’s ToS field, the packet will go to one of four outbound port queues in the switch: 1 - 2 = low priority 0 - 3 = normal priority 4 - 5 = high priority 6 - 7 = high priority</td>
</tr>
<tr>
<td>IP Packet in a Tagged VLAN</td>
<td>Same as above, plus the IP Precedence value (0 - 7) will be used to set a corresponding 802.1p priority in the VLAN tag carried by the packet to the next downstream device.</td>
</tr>
</tbody>
</table>
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

QoS LAN Protocol Priority

QoS Classifier Precedence: 4

The QoS protocol option enables you to use these protocols as QoS classifiers:

- IP
- ARP
- Appletalk
- Netbeui
- IPX
- DEC_LAT
- SNA

Options for Assigning Priority. Priority control for the LAN protocol classifier includes assigning only the 802.1p priority. The switch does not use this classifier for assigning DSCP-based priority.

Assigning a Priority Based on LAN Protocol

When QoS on the switch is configured with a LAN protocol as the highest-precedence classifier and the switch receives traffic carrying that protocol, then this traffic is assigned the priority configured for this classifier. (For operation when other QoS classifiers apply to the same traffic, refer to “Classifiers for Prioritizing Outbound Packets” on page 8-8.)

Syntax: qos protocol

< ip | ipx | arp | dec_lat | appletalk | sna | netbeui > priority < 0 - 7 >

Configures an 802.1p priority for outbound packets having the specified protocol. This priority determines the packet’s queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. You can configure one QoS classifier for each protocol type. (Default: No-override)

no qos protocol

< ip | ipx | arp | dec_lat | appletalk | sna | netbeui >

Disables use of the specified protocol as a QoS classifier and resets the protocol priority to No-override.

show qos protocol

Lists the QoS protocol classifiers with their priority settings.
For example:

1. Configure QoS protocol classifiers with IP at 0 (normal), ARP at 5 (medium), and AppleTalk at 7 (high) and display the QoS protocol configuration.

2. Disable the QoS IP protocol classifier, downgrade the ARP priority to 4, and again display the QoS protocol configuration.

Figure 8-19 shows the command sequence and displays for the above steps.

```
HPswitch(config)# qos protocol ip priority 0
HPswitch(config)# qos protocol appleTalk priority 7
HPswitch(config)# qos protocol arp priority 5

HPswitch(config)# show qos protocol
Protocol priorities
--- ---------
Protocol  Priority
-----------
  IP        0
  IPX       No-override
  ARP       5
  DEC_LAT   No-override
  AppleTalk 7
  SNA       No-override
  NetBEUI   No-override

HPswitch(config)# no qos protocol ip
HPswitch(config)# qos protocol arp priority 4

HPswitch(config)# show qos protocol
Protocol priorities
--- ---------
Protocol  Priority
-----------
  IP        No-override
  IPX       No-override
  ARP       4
  DEC_LAT   No-override
  AppleTalk 7
  SNA       No-override
  NetBEUI   No-override
```

Figure 8-19. Adding, Displaying, Removing, and Changing QoS Protocol Classifiers
QoS VLAN-ID (VID) Priority

QoS Classifier Precedence: 5

The QoS protocol option enables you to use up to 256 VLAN-IDs as QoS classifiers. Where a particular VLAN-ID classifier has the highest precedence in the switch for traffic in that VLAN, then traffic received in that VLAN is marked with the VID classifier's configured priority level. Different VLAN-ID classifiers can have differing priority levels.

Options for Assigning Priority. Priority control options for packets carrying a specified VLAN-ID include:

- 802.1p priority
- DSCP policy (Assigning a new DSCP and an associated 802.1p priority; inbound packets must be IPv4.)

(For operation when other QoS classifiers apply to the same traffic, refer to “Classifiers for Prioritizing Outbound Packets” on page 8-8.)

**Note**

QoS with VID priority applies to static VLANs only, and applying QoS to dynamic VLANs created by GVRP operation is not supported. A VLAN must exist while a subject of a QoS configuration, and eliminating a VID from the switch causes the switch to clear any QoS features configured for that VID.

Assigning a Priority Based on VLAN-ID Only

This option assigns a priority to all outbound packets having the specified VLAN-ID (VID). You can configure this option by either specifying the VLAN-ID ahead of the `qos` command or moving to the VLAN context for the VLAN you want to configure for priority.

Syntax: `vlan <vlan-id> qos priority <0-7>

Configures an 802.1p priority for outbound packets belonging to the specified VLAN. This priority determines the packet's queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. You can configure one QoS classifier for each VLAN-ID. (Default: No-override)
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

no vlan <vlan-id> qos

Removes the specified VLAN-ID as a QoS classifier and resets the priority for that VLAN to No-override.

show qos vlan-priority

Displays a listing of the QoS VLAN-ID classifiers currently in the running-config file, with their priority data.

1. For example, suppose that you have the following VLANs configured on the switch and want to prioritize them as shown:

```
HPswitch(config)# show vlan
Status and Counters - VLAN Information
Maximum VLANs to support : 8
Primary VLAN : DEFAULT_VLAN

<table>
<thead>
<tr>
<th>Set Priority To</th>
<th>802.1Q VLAN ID</th>
<th>Name</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Priority To 2</td>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>VLAN_20</td>
<td>Static</td>
</tr>
<tr>
<td>Set Priority To 5</td>
<td>20</td>
<td>VLAN_30</td>
<td>Static</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>VLAN_40</td>
<td>Static</td>
</tr>
</tbody>
</table>
```

Figure 8-20. Example of a List of VLANs Available for QoS Prioritization

2. You would then execute the following commands to prioritize the VLANs by VID:

```
HPswitch(config)# vlan 1 qos priority 2
HPswitch(config)# vlan 20 qos priority 5
HPswitch(config)# vlan 30 qos priority 5
HPswitch(config)# vlan 40 qos priority 7

HPswitch(config)# show qos vlan
VLAN priorities

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Priority</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Priority</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Priority</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>Priority</td>
<td>7</td>
<td></td>
</tr>
</tbody>
</table>
```

Figure 8-21. Configuring and Displaying QoS Priorities on VLANs
If you then decided to remove VLAN_20 from QoS prioritization:

```
HPswitch(config)# no vlan 20 qos
HPswitch(config)# show qos vlan
```

![Figure 8-22. Returning a QoS-Prioritized VLAN to “No-override” Status](image)

**Assigning a DSCP Policy Based on VLAN-ID (VID)**

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets having the specified VLAN-ID (VID). That is, the switch:

1. Selects an incoming IP packet on the basis of the VLAN-ID it carries.
2. Overwrites the packet’s DSCP with the DSCP configured in the switch for such packets.
3. Assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)
4. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, refer to “Terminology” on page 8-5.

**Steps for Creating a Policy Based on VLAN-ID Classifier.**

1. Determine the VLAN-ID classifier to which you want to assign a DSCP policy.
2. Determine the DSCP policy for packets carrying the selected VLAN-ID:
   a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite the DSCP carried in packets received from upstream devices.)
   b. Determine the 802.1p priority you want to assign to the DSCP.
3. Configure the DSCP policy by using `qos dscp-map` to configure the priority for each codepoint. (For details, see the example later in this section, and to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)
A codepoint must have an 802.1p priority (0 - 7) before you can configure the codepoint for use in prioritizing packets by VLAN-ID. If a codepoint you want to use shows No-override in the Priority column of the DSCP Policy table (show qos dscp-map), then assign a priority before proceeding.

4. Configure the switch to assign the DSCP policy to packets with the specified VLAN-ID.

**Syntax:** qos dscp-map <codepoint> priority <0 - 7>

This command is optional if a priority has already been assigned to the <codepoint>. The command creates a DSCP policy by assigning an 802.1p priority to a specific DSCP. When the switch applies this priority to a packet, the priority determines the packet’s queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. If the packet is IPv4, the packet’s DSCP will be replaced by the codepoint specified in this command. (Default: For most codepoints, No-override. See figure 8-8-6 on page 8-51.)

**Syntax:** vlan <vid> qos dscp <codepoint>

Assigns a DSCP policy to packets carrying the specified IP address, and overwrites the DSCP in these packets with the assigned <codepoint> value. This policy includes an 802.1p priority and determines the packet’s queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. (Default: No-override)

no vlan <vid> qos

Removes QoS classifier for the specified VLAN.

show qos device-priority

Displays a listing of all QoS VLAN-ID classifiers currently in the running-config file.
For example, suppose you wanted to assign this set of priorities:

<table>
<thead>
<tr>
<th>VLAN-ID</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>000111</td>
<td>7</td>
</tr>
<tr>
<td>30</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>20</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>000010</td>
<td>1</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP. (Refer to the “Note On Changing a Priority Setting” on page 8-53. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

```
HPswitch(config)# show qos dscp-map
DSCP -> 802.p priority mappings
DSCP policy 802.1p tag Policy name
---------- ---------- -------------
000000     No-override
000001     No-override
000010     No-override
000011     No-override
000100     No-override
000101     No-override
000110     No-override
000111     No-override
          ...
```

The DSCPs for this example have not yet been assigned an 802.1p priority level.

**Figure 8-23. Display the Current Configuration in the DSCP Policy Table**

2. Configure the priorities for the DSCPs you want to use.

```
HPswitch(config)# qos dscp-map 000111 priority 7
HPswitch(config)# qos dscp-map 000101 priority 5
HPswitch(config)# qos dscp-map 000010 priority 1
HPswitch(config)# show qos dscp-map
DSCP -> 802.p priority mappings
DSCP policy 802.1p tag Policy name
---------- ---------- -------------
000000     No-override
000001     No-override
000010     1
000011     No-override
000100     No-override
000101     5
000110     No-override
000111     7
001000     No-override
          ...
```

**Figure 8-24. Assign Priorities to the Selected DSCPs**
3. Assign the DSCP policies to the selected VIDs and display the result.

```
HPswitch(config)# vlan 1 qos dscp 000010
HPswitch(config)# vlan 20 qos dscp 000010
HPswitch(config)# vlan 30 qos dscp 000101
HPswitch(config)# vlan 40 qos dscp 000111
```

```
HPswitch(config)# show qos vlan-priority

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>20</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>30</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>DSCP</td>
<td>000111</td>
<td>7</td>
</tr>
</tbody>
</table>
```

**Figure 8-25. The Completed VID-DSCP Priority Configuration**

The switch will now apply the DSCP policies in figure 8-25 to packets received on the switch with the specified VLAN-IDs. This means the switch will:

- Overwrite the original DSCPs in the selected packets with the new DSCPs specified in the above policies.
- Assign the 802.1p priorities in the above policies to the appropriate packets.

**QoS Source-Port Priority**

**QoS Classifier Precedence: 6**

The QoS source-port option enables you to use a packet’s source-port on the switch as a QoS classifier. Where a particular source-port classifier has the highest precedence in the switch for traffic entering through that port, then traffic received from the port is marked with the source-port classifier’s configured priority level. Different source-port classifiers can have different priority levels.
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

**Options for Assigning Priority.** Priority control options for packets from a specified source-port include:

- **802.1p priority**
- **DSCP policy** (Assigning a new DSCP and an associated 802.1p priority; inbound packets must be IPv4.)

(For operation when other QoS classifiers apply to the same traffic, refer to “Classifiers for Prioritizing Outbound Packets” on page 8-8.)

**Assigning a Priority Based on Source-Port Only**

This option assigns a priority to all outbound packets having the specified source-port. You can configure this option by either specifying the source-port ahead of the qos command or moving to the port context for the port you want to configure for priority. (If you are configuring multiple source-ports with the same priority, you may find it easier to use the port context instead of individually configuring the priority for each port.)

**Syntax:**

```
interface < port-list > qos priority < 0 - 7 >
```

Configures an 802.1p priority for outbound packets entering the switch through the specified (source) ports. This priority determines the packet queue in the outbound port(s) to which traffic from the source-ports is sent. If a packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. You can configure one QoS classifier for each source-port or group of source-ports. (Default: No-override)

```
no interface < port-list > qos
```

Disables use of the specified source-port(s) for QoS classifier(s) and resets the priority for the specified source-port(s) to No-override.

```
show qos vlan-priority
```

Lists the QoS VLAN-ID classifiers with their priority data.
For example, suppose that you want to prioritize inbound traffic on the following source-ports:

<table>
<thead>
<tr>
<th>Source-Port</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 - A3</td>
<td>2</td>
</tr>
<tr>
<td>A4</td>
<td>3</td>
</tr>
<tr>
<td>B1, B4</td>
<td>5</td>
</tr>
<tr>
<td>C1-C3</td>
<td>6</td>
</tr>
</tbody>
</table>

You would then execute the following commands to prioritize traffic received on the above ports:

```bash
HPswitch(config)# interface e c1-c3 qos priority 6
HPswitch(config)# interface e b1,b4 qos priority 5
HPswitch(config)# interface e a4 qos priority 3
HPswitch(config)# interface e a1-a3 qos priority 2
HPswitch(config)# show qos port-priority
```

If you then decided to remove port A1 from QoS prioritization:

```bash
HPswitch(config)# no interface e a1 qos
HPswitch(config)# show qos port-priority
```

In this instance, **No-override** indicates that port A1 is not prioritized by QoS.
Assigning a DSCP Policy Based on the Source-Port

This option assigns a previously configured DSCP policy (codepoint and 802.1p priority) to outbound IP packets (received from the specified source-ports). That is, the switch:

1. Selects an incoming IP packet on the basis of its source-port on the switch.
2. Overwrites the packet’s DSCP with the DSCP configured in the switch for such packets.
3. Assigns the 802.1p priority configured in the switch for the new DSCP. (Refer to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)
4. Forwards the packet through the appropriate outbound port queue.

For more on DSCP, refer to “Terminology” on page 8-5.

Steps for Creating a Policy Based on Source-Port Classifiers.

---

**Note**

You can select one DSCP per source-port. Also, configuring a new DSCP for a source-port automatically overwrites (replaces) any previous DSCP or 802.1p priority configuration for that port.

1. Identify the source-port classifier to which you want to assign a DSCP policy.
2. Determine the DSCP policy for packets having the selected source-port:
   a. Determine the DSCP you want to assign to the selected packets. (This codepoint will be used to overwrite the DSCP carried in packets received through the source-port from upstream devices.)
   b. Determine the 802.1p priority you want to assign to the DSCP.
3. Configure the DSCP policy by using `qos dscp-map` to configure the priority for each codepoint. (For details, refer to the example later in this section and to “Differentiated Services Codepoint (DSCP) Mapping” on page 8-50.)

---

**Note**

A codepoint must have an 802.1p priority assignment (0 - 7) before you can configure that codepoint as a criteria for prioritizing packets by source-port. If a codepoint shows **No-override** in the Priority column of the DSCP Policy Table (`show qos dscp-map`), then you must assign a 0 - 7 priority before proceeding.
4. Configure the switch to assign the DSCP policy to packets from the specified source-port.

**Syntax:** `qos dscp-map < codepoint > priority < 0 - 7 >`

*This command is optional if a priority has already been assigned to the <codepoint>. The command creates a DSCP policy by assigning an 802.1p priority to a specific DSCP. When the switch applies this priority to a packet, the priority determines the packet’s queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. (Default: For most codepoints, **No-override**. See figure 8-8-6 on page 8-51.)*

**Syntax:** `interface < port-list > qos dscp < codepoint >`

*Assigns a DSCP policy to packets from the specified source-port(s), and overwrites the DSCP in these packets with the assigned <codepoint> value. This policy includes an 802.1p priority and determines the packet’s queue in the outbound port to which it is sent. If the packet leaves the switch in a tagged VLAN, it carries the 802.1p priority with it to the next downstream device. (Default: **No-override**)*

no interface [e] < port-list > qos

*Removes QoS classifier for the specified source-port(s).*

show qos source-port

*Displays a listing of all source-port QoS classifiers currently in the running-config file.*
For example, suppose you wanted to assign this set of priorities:

<table>
<thead>
<tr>
<th>Source-Port</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2</td>
<td>000111</td>
<td>7</td>
</tr>
<tr>
<td>B1-B3</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>B4, C2</td>
<td>000010</td>
<td>1</td>
</tr>
</tbody>
</table>

1. Determine whether the DSCPs already have priority assignments, which could indicate use by existing applications. This is not a problem as long as the configured priorities are acceptable for all applications using the same DSCP. (Refer to the “Note On Changing a Priority Setting” on page 8-53. Also, a DSCP must have a priority configured before you can assign any QoS classifiers to use it.)

2. Configure the priorities for the DSCPs you want to use.
3. Assign the DSCP policies to the selected source-ports and display the result.

```
HPswitch(eth-A2)# int e b4,c2
HPswitch(eth-B4,C2)# qos dscp 000010
HPswitch(eth-B4,C2)# int e b1-b3
HPswitch(eth-B1-B3)# qos dscp 000101
HPswitch(eth-B1-B3)# int e a2
HPswitch(eth-A2)# qos dscp 000111

HPswitch(eth-A2)# show qos port-priority
Port priorities
<table>
<thead>
<tr>
<th>Port</th>
<th>Apply rule</th>
<th>DSCP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2</td>
<td>No-override</td>
<td>000111</td>
<td>7</td>
</tr>
<tr>
<td>A3</td>
<td>No-override</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>A4</td>
<td>No-override</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>B1</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>B2</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>B3</td>
<td>DSCP</td>
<td>000101</td>
<td>5</td>
</tr>
<tr>
<td>B4</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>C1</td>
<td>No-override</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>C2</td>
<td>DSCP</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>C3</td>
<td>No-override</td>
<td>000010</td>
<td>1</td>
</tr>
<tr>
<td>C4</td>
<td>No-override</td>
<td>000010</td>
<td>1</td>
</tr>
</tbody>
</table>
```

Figure 8-30. The Completed Source-Port DSCP-Priority Configuration
Differentiated Services Codepoint (DSCP) Mapping

The DSCP Policy Table associates an 802.1p priority with a specific ToS byte codepoint in an IPv4 packet. This enables you to set a LAN policy that operates independently of 802.1Q VLAN-tagging.

In the default state, most of the 64 codepoints do not assign an 802.1p priority, as indicated by No-override in table 8-6 on page 8-51.

You can list the current DSCP Policy table, change the codepoint priority assignments, and assign optional names to the codepoints.

**Syntax:**

```
show qos dscp-map

qos dscp-map < codepoint > priority < 0 - 7 > [name < ascii-string >]

no qos dscp-map < codepoint >

no qos dscp-map < codepoint > name
```

*Displays the DSCP Policy Table.*

*Configures an 802.1p priority for the specified codepoint and, optionally, an identifying (policy) name.*

*Reconfigures the 802.1p priority for <codepoint> to No-override. Also deletes the codepoint policy name, if configured.*

*Deletes only the policy name, if configured, for <codepoint>.*
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

Table 8-6. The Default DSCP Policy Table

<table>
<thead>
<tr>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
<th>DSCP Policy</th>
<th>802.1p Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>000000</td>
<td>No-override</td>
<td>010110</td>
<td>3</td>
<td>101011</td>
<td>No-override</td>
</tr>
<tr>
<td>000001</td>
<td>No-override</td>
<td>010111</td>
<td>No-override</td>
<td>101100</td>
<td>No-override</td>
</tr>
<tr>
<td>000010</td>
<td>No-override</td>
<td>011000</td>
<td>No-override</td>
<td>101101</td>
<td>No-override</td>
</tr>
<tr>
<td>000011</td>
<td>No-override</td>
<td>011001</td>
<td>No-override</td>
<td>101110</td>
<td>7</td>
</tr>
<tr>
<td>000100</td>
<td>No-override</td>
<td>011010</td>
<td>4</td>
<td>101111</td>
<td>No-override</td>
</tr>
<tr>
<td>000101</td>
<td>No-override</td>
<td>011101</td>
<td>No-override</td>
<td>110000</td>
<td>No-override</td>
</tr>
<tr>
<td>000110</td>
<td>No-override</td>
<td>011100</td>
<td>4</td>
<td>110001</td>
<td>No-override</td>
</tr>
<tr>
<td>000111</td>
<td>No-override</td>
<td>011101</td>
<td>No-override</td>
<td>110010</td>
<td>No-override</td>
</tr>
<tr>
<td>001000</td>
<td>No-override</td>
<td>011110</td>
<td>5</td>
<td>110011</td>
<td>No-override</td>
</tr>
<tr>
<td>001001</td>
<td>No-override</td>
<td>011111</td>
<td>No-override</td>
<td>110100</td>
<td>No-override</td>
</tr>
<tr>
<td>001010</td>
<td>1</td>
<td>100000</td>
<td>No-override</td>
<td>110101</td>
<td>No-override</td>
</tr>
<tr>
<td>001011</td>
<td>No-override</td>
<td>100001</td>
<td>No-override</td>
<td>110110</td>
<td>No-override</td>
</tr>
<tr>
<td>001100</td>
<td>1</td>
<td>100010</td>
<td>6</td>
<td>110111</td>
<td>No-override</td>
</tr>
<tr>
<td>001101</td>
<td>No-override</td>
<td>100011</td>
<td>No-override</td>
<td>111000</td>
<td>No-override</td>
</tr>
<tr>
<td>001110</td>
<td>2</td>
<td>100100</td>
<td>6</td>
<td>111001</td>
<td>No-override</td>
</tr>
<tr>
<td>001111</td>
<td>No-override</td>
<td>100101</td>
<td>No-override</td>
<td>111010</td>
<td>No-override</td>
</tr>
<tr>
<td>010000</td>
<td>No-override</td>
<td>100110</td>
<td>7</td>
<td>111011</td>
<td>No-override</td>
</tr>
<tr>
<td>010001</td>
<td>No-override</td>
<td>100111</td>
<td>No-override</td>
<td>111100</td>
<td>No-override</td>
</tr>
<tr>
<td>010010</td>
<td>0</td>
<td>101000</td>
<td>No-override</td>
<td>111101</td>
<td>No-override</td>
</tr>
<tr>
<td>010011</td>
<td>No-override</td>
<td>101001</td>
<td>No-override</td>
<td>111110</td>
<td>No-override</td>
</tr>
<tr>
<td>010100</td>
<td>0</td>
<td>101010</td>
<td>No-override</td>
<td>111111</td>
<td>No-override</td>
</tr>
<tr>
<td>010101</td>
<td>No-override</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Default Priority Settings for Selected Codepoints

In a few cases, such as 001010 and 001100, a default policy (implied by the DSCP standards for Assured-Forwarding and Expedited-Forwarding) is used. You can change the priorities for the default policies by using `qos dscp-map <codepoint> priority <0 - 7>`.(These policies are not in effect unless you have either applied the policies to a QoS classifier or configured QoS Type-of-Service to be in `diff-services` mode.)

Quickly Listing Non-Default Codepoint Settings

Table 8-6 lists the switch's default codepoint/priority settings. If you change the priority of any codepoint setting to a non-default value and then execute `write memory`, the switch will list the non-default setting in the show config display. For example, in the default configuration, the following codepoint settings are true:
Quality of Service (QoS): Managing Bandwidth More Effectively
Using QoS Classifiers To Configure Quality of Service for Outbound Traffic

<table>
<thead>
<tr>
<th>Codepoint</th>
<th>Default Priority</th>
<th>No-override</th>
</tr>
</thead>
<tbody>
<tr>
<td>001100</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>001101</td>
<td>No-override</td>
<td></td>
</tr>
<tr>
<td>001110</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

If you change all three settings to a priority of 3, and then execute `write memory`, the switch will reflect these changes in the show config listing:

```
 HPswitch(config)# qos dscp-map 001100 priority 3
 HPswitch(config)# qos dscp-map 001101 priority 3
 HPswitch(config)# qos dscp-map 001110 priority 3
 HPswitch(config)# write memory
 HPswitch(config)# show config

startup configuration:
hostname "HPswitch"

---

HPswitch(config)# show config

: J4850A Configuration Editor; Created on release #E.05.01

hostname "HPswitch"

---

qos dscp-map 001100 priority 3
qos dscp-map 001101 priority 3
qos dscp-map 001110 priority 3
module 2 type J4821A
module 3 type J4820A
```

Figure 8-31. Example of Show Config Listing with Non-Default Priority Settings in the DSCP Table

**Effect of “No-override”**. In the QoS Type-of-Service differentiated services mode, a **No-override** assignment for the codepoint of an outbound packet means that QoS is effectively disabled for such packets. That is, QoS does not affect the packet queuing priority or VLAN tagging. In this case, the packets are handled as follows (as long as no other QoS feature creates priority assignments for them):

<table>
<thead>
<tr>
<th>802.1Q Status</th>
<th>Outbound 802.1p Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received and Forwarded on a tagged VLAN</td>
<td>Unchanged</td>
</tr>
<tr>
<td>Received on an Untagged VLAN; Forwarded on a tagged VLAN</td>
<td>0 (zero)—“normal”</td>
</tr>
<tr>
<td>Forwarded on an Untagged VLAN</td>
<td>None</td>
</tr>
</tbody>
</table>
Note On Changing a Priority Setting

If a QoS classifier is using a policy (codepoint and associated priority) in the DSCP Policy table, you must delete or change this usage before you can change the priority setting on the codepoint. Otherwise the switch blocks the change and displays this message:

**Cannot modify DSCP Policy < codepoint > - in use by other qos rules.**

In this case, use `show qos < classifier>` to identify the specific classifiers using the policy you want to change; that is:

- `show qos device-priority`
- `show qos port-priority`
- `show qos tcp-udp-port-priority`
- `show qos vlan-priority`
- `show qos type-of-service`

Note that protocol-priority is not included because a DSCP policy is not meaningful for this classifier and therefore not configurable in this case.

For example, suppose that the 000001 codepoint has a priority of 6, and several classifiers use the 000001 codepoint to assign a priority to their respective types of traffic. If you wanted to change the priority of codepoint 000001 you would do the following:

1. Identify which QoS classifiers use the codepoint.
2. Change the classifier configurations by assigning them to a different DSCP policy, or to an 802.1p priority, or to **No-override**.
3. Reconfigure the desired priority for the 000001 codepoint.
4. Either reassign the classifiers to the 00001 codepoint policy or leave them as they were after step 2, above.

Example of Changing the Priority Setting on a Policy When One or More Classifiers Are Currently Using the Policy

Suppose that codepoint 000001 is in use by one or more classifiers. If you try to change its priority, you see a result similar to the following:

```
HPswitch(config)# qos dscp-map 000001 priority 2
Cannot modify DSCP Policy 000001 - in use by other qos rules.
```

**Figure 8-32. Example of Trying To Change the Priority on a Policy In Use by a Classifier**

In this case, you would use steps similar to the following to change the priority.
1. Identify which classifiers use the codepoint you want to change.

---

**Figure 8-33. Example of a Search to Identify Classifiers Using a Codepoint You Want To Change**
2. Change the classifier configurations by assigning them to a different DSCP policy, or to an 802.1p priority, or to No-override. For example:
   a. Delete the policy assignment for the device-priority classifier. (That is, assign it to No-override.)
   b. Create a new DSCP policy to use for re-assigning the remaining classifiers.
   c. Assign the port-priority classifier to the new DSCP policy.
   d. Assign the udp-port 1260 classifier to an 802.1p priority.

   a) HPswitch(config)# no qos device-priority 10.26.50.104
   b) HPswitch(config)# qos dscp-map 000100 priority 6
   c) HPswitch(config)# int e a3 qos dscp 000100
   d) HPswitch(config)# qos udp-port 1260 priority 2

3. Reconfigure the desired priority for the 000001 codepoint.
   HPswitch(config)# qos dscp-map 000001 priority 4

4. You could now re-assign the classifiers to the original policy codepoint or leave them as currently configured.
Configuring QoS from the Web Browser Interface

1. Click here.
2. Click here.

The default screen displays the TCP/UDP Application Priority option.

![Figure 8-34. The Default QoS Configuration Screen](image-url)
IP Multicast (IGMP) Interaction with QoS

IGMP high-priority-forward causes the switch to service the subscribed IP multicast group traffic at high priority, even if QoS on the switch has relegated the traffic to a lower priority. This does not affect any QoS priority settings, so the QoS priority is honored by downstream devices. However, QoS does take precedence over IGMP normal-priority traffic.

The switch’s ability to prioritize IGMP traffic for either a normal or high priority outbound queue overrides any QoS criteria, and does not affect any 802.1p priority settings the switch may assign. For a given packet, if both IGMP high priority and QoS are configured, the QoS classification occurs and the switch marks the packet for downstream devices, but the packet is serviced by the high-priority queue when leaving the switch.

<table>
<thead>
<tr>
<th>IGMP High Priority</th>
<th>QoS Configuration Affects Packet</th>
<th>Switch Port Output Queue</th>
<th>Outbound 802.1p Setting (Requires Tagged VLAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not Enabled</td>
<td>Yes</td>
<td>Determined by QoS</td>
<td>Determined by QoS</td>
</tr>
<tr>
<td>Enabled</td>
<td>See above paragraph</td>
<td>High</td>
<td>As determined by QoS if QoS is active.</td>
</tr>
</tbody>
</table>

QoS Messages in the CLI

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP Policy &lt; decimal-codepoint &gt; not configured-</td>
<td>You have attempted to map a QoS classifier to a codepoint for which there is no configured priority (No-override). Use the qos dscp-map command to configure a priority for the codepoint, then map the classifier to the codepoint.</td>
</tr>
<tr>
<td>Cannot modify DSCP Policy &lt; codepoint &gt; - in use by other qos rules.</td>
<td>You have attempted to map a QoS classifier to a codepoint that is already in use by other QoS classifiers. Before remapping the codepoint to a new priority, you must reconfigure the other QoS classifiers so that they do not use this codepoint. You can have multiple QoS classifiers use this same codepoint as long as it is acceptable for all such classifiers to use the same priority.</td>
</tr>
</tbody>
</table>
QoS Operating Notes

- For Devices that Do Not Support 802.1Q Tagged VLANs: For communication between these devices and the switch, connect the device to a switch port configured as UnTagged for the VLAN in which you want the device’s traffic to move.

- VLAN Tagging Rules: For a port on the switch to be a member of a VLAN, the port must be configured as either Tagged or UnTagged for that VLAN. (Only one VLAN on a port can be untagged. Otherwise, the switch cannot determine which VLAN should receive untagged VLAN traffic.)

- Maximum QoS Configuration Entries: Beginning with software release E.08.xx, the switch allows up to 400 QoS outbound priority and/or DSCP policy configuration entries. Attempting to exceed this limit generates the following message in the CLI:

  Unable to add this QoS rule. Maximum number (400) already reached.

  Where the switch is running a software release earlier than E.08.xx and is configured with more than 400 QoS rules, downloading software release E.08.xx (or greater) causes the switch to:
  - Implement the first 400 QoS rules in its configuration, but ignore the configured rules exceeding that limit.
  - Generate these Event Log messages:
    - Too many QoS configuration items - limit of 400
    - Some QoS configuration items will not be active
Access Control Lists (ACLs)

Contents

Introduction ................................................................. 9-3
Terminology ................................................................. 9-5
Overview ................................................................. 9-8
  Types of IP ACLs ................................................... 9-8
  ACL Inbound and Outbound Application Points ............ 9-8
  Features Common to All ACLs .............................. 9-9
  General Steps for Planning and Configuring ACLs .... 9-10
ACL Operation ................................................................. 9-12
  Introduction .......................................................... 9-12
  The Packet-Filtering Process ............................... 9-13
Planning an ACL Application ........................................ 9-16
  Traffic Management and Improved Network Performance 9-16
  Security .............................................................. 9-17
  Guidelines for Planning the Structure of an ACL .... 9-18
  ACL Configuration and Operating Rules .................. 9-18
  How an ACE Uses a Mask To Screen Packets for Matches 9-20
    What Is the Difference Between Network (or Subnet) Masks
    and the Masks Used with ACLs? .......................... 9-20
    Rules for Defining a Match Between a Packet and an
    Access Control Entry (ACE) .................................. 9-21
Configuring and Assigning an ACL ................................. 9-25
  Overview .......................................................... 9-25
  General Steps for Implementing ACLs ..................... 9-25
  Types of ACLs .................................................... 9-26
  ACL Configuration Structure .................................. 9-26
  Standard ACL Structure ......................................... 9-27
  Extended ACL Configuration Structure .................... 9-28
  ACL Configuration Factors .................................. 9-29
The Sequence of Entries in an ACL Is Significant ................. 9-29
In Any ACL, There Will Always Be a Match ....................... 9-31
A Configured ACL Has No Effect Until You Apply It to an
Interface ......................................................................... 9-31
Using the CLI To Create an ACL ......................................... 9-31
General ACE Rules .......................................................... 9-32
Using CIDR Notation To Enter the ACL Mask ...................... 9-32
Configuring and Assigning a Numbered, Standard ACL ........ 9-33
Configuring and Assigning a Numbered, Extended ACL ....... 9-38
Configuring a Named ACL .................................................. 9-44
Enabling or Disabling ACL Filtering on a VLAN ................. 9-46

Deleting an ACL from the Switch ........................................ 9-47

Displaying ACL Data ...................................................... 9-48
Display an ACL Summary .................................................. 9-48
Display the Content of All ACLs on the Switch .................... 9-49
Display the ACL Assignments for a VLAN ......................... 9-50
Displaying the Content of a Specific ACL ......................... 9-51
Display All ACLs and Their Assignments in the Switch
Start-up-Config File and Running-Config File .................... 9-53

Editing ACLs and Creating an ACL Offline ......................... 9-53
Using the CLI To Edit ACLs .............................................. 9-53
General Editing Rules ...................................................... 9-54
Deleting Any ACE from an ACL ......................................... 9-54
Working Offline To Create or Edit an ACL ......................... 9-56

Enable ACL “Deny” Logging .............................................. 9-59
Requirements for Using ACL Logging ................................. 9-59
ACL Logging Operation ...................................................... 9-60
Enabling ACL Logging on the Switch ................................. 9-60
Operating Notes for ACL Logging ....................................... 9-62

General ACL Operating Notes ........................................... 9-63
Layer 3 IP filtering with Access Control Lists (ACLs) on the HP Series 5300XL switches enables you to improve network performance and restrict network use by creating policies for:

- **Switch Management Access:** Permits or denies in-band management access. This includes preventing the use of certain TCP or UDP applications (such as Telnet, SSH, web browser, and SNMP) for transactions between specific source and destination IP addresses.

- **Application Access Security:** Eliminates unwanted IP, TCP, or UDP traffic in a path by filtering packets where they enter or leave the switch on specific VLAN interfaces.

ACLs can filter traffic to or from a host, a group of hosts, or entire subnets.

This chapter describes how to configure, apply, and edit ACLs in a network populated with HP Series 5300XL switches (with IP routing support enabled) and how to monitor the results of ACL actions.

**Notes**

ACLs can enhance network security by blocking selected IP traffic, and can serve as one aspect of maintaining network security. However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.

ACLs in the Series 5300XL switches do not screen non-IP traffic such as AppleTalk and IPX.
For ACL filtering to take effect, configure an ACL and then assign it to either the inbound or outbound traffic on a statically configured VLAN on the switch. (Except for ACEs that screen traffic to an IP address on the switch itself, ACLs assigned to VLANs can operate only while IP routing is enabled. Refer to “Notes on IP Routing” on page 9-11.)

Table 9-1. Comprehensive Command Summary

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Standard</td>
<td>HPswitch(config)# [no] access-list &lt; 1-99 &gt; &lt; deny</td>
<td>permit &gt;</td>
</tr>
<tr>
<td>(Numbered) ACLs</td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
|                               | < any | host < src-ip-addr > | src-ip-address/mask >  
|                               | [log]²                                                                 |      |
| Configuring Extended          | HPswitch(config)# [no] access-list <100-199> < deny | permit >                               | 9-3  |
| (Numbered) ACLs               |                                                                         | 8    |
|                               | ip < any | host < src-ip-addr > | src-ip-address/mask >  
|                               | [log]²                                                                 |      |
|                               | HPswitch(config)# [no] access-list < 100-199 > < deny | permit >                             |      |
|                               | < tcp | udp >                                                |      |
|                               | < any | host < src-ip-addr > | src-ip-address/mask >  
|                               | [operator < src-port tcp/udp-id >]                  |      |
|                               | < any | host < dest-ip-addr > | dest-ip-address/mask >  
|                               | [operator < dest-port tcp/udp-id >]                 |      |
|                               | [log]²                                                                 |      |
| Configuring Standard          | HPswitch(config)# [no] ip access-list standard < name-str | 1-99 >                               | 9-4  |
| (Named) ACLs                  |                                                                         | 4    |
|                               | HPswitch(config-std-nacl)# < deny | permit >                               |      |
|                               | < any | host < src-ip-addr > | src-ip-address/mask >  
|                               | [log]²                                                                 |      |
| Configuring Extended          | HPswitch(config)# [no] ip access-list extended < name-str | 100-199 >                             |      |
| (Named) ACLs                  |                                                                         |      |
|                               | HPswitch(config-std-nacl)# < deny | permit > ip                             |      |
|                               | < any | host < src-ip-addr > | src-ip-address/mask >  
|                               | < any | host < dest-ip-addr > | dest-ip-address/mask >  
|                               | [log]²                                                                 |      |
|                               | HPswitch(config-std-nacl)# < deny | permit > < tcp | udp >                        |      |
|                               | < any | host < src-ip-addr > | src-ip-address/mask >  
|                               | [operator < src-port tcp/udp-id >]                  |      |
|                               | < any | host < dest-ip-addr > | dest-ip-address/mask >  
|                               | [operator < dest-port tcp/udp-id >]                 |      |
|                               | [log]²                                                                 |      |
| Enabling or Disabling         | HPswitch(config)# [no] vlan < vid > ip access-group                  | 9-4  |
| an ACL                        |                                                                         | 6    |
|                               | < name-str | 1-99 | 100-199 > < in | out >                  |      |

¹The mask can be in either dotted-decimal notation (such as 0.0.15.255) or CIDR notation (such as /20).
²The [log] function applies only to “deny” ACLs, and generates a message only when there is a “deny” match.
### Terminology

**Access Control Entry (ACE):** An ACE is a policy consisting of criteria and an action to take (permit or deny) on a packet if it meets the criteria. The elements composing the criteria include:

- Source IP address and mask (standard and extended ACLs)
- Destination IP address and mask (extended ACLs only)
- TCP or UDP application port numbers (optional, extended ACLs only)

**Access Control List (ACL):** A list (or set) consisting of one or more explicitly configured Access Control Entries (ACEs) and terminating with an implicit “deny” default which drops any packets that do not have a match with any explicit ACE in the named ACL. The two classes of ACLs are “standard” and “extended”. See “Standard ACL” and “Extended ACL”.

**ACE:** See “Access Control Entry”.

**ACL:** See “Access Control List”.

**ACL ID:** A number or alphanumeric string used to identify an ACL. A *standard* ACL ID can have either a number from 1 to 99 or an alphanumeric string. An *extended* ACL ID can have either a number from 100 to 199 or an alphanumeric string.

---

<table>
<thead>
<tr>
<th>Action</th>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleting an ACL from the Switch</td>
<td>HPswitch(config)# no ip access-list &lt; standard</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>out &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt; name-str</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt; in</td>
</tr>
<tr>
<td>Displaying ACL Data</td>
<td>HPswitch(config)# show access-list</td>
<td>9-4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HPswitch(config)# show access-list config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HPswitch(config)# show access-list vlan &lt; vid &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HPswitch(config)# show config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HPswitch(config)# show running</td>
</tr>
</tbody>
</table>

---
**Access Control Lists (ACLs)**

**Terminology**

**ACL Mask:** Follows any IP address (source or destination) listed in an ACE. Defines which bits in a packet’s corresponding IP addressing must exactly match the IP addressing in the ACE, and which bits need not match (wildcards). See also “How an ACE Uses a Mask To Screen Packets for Matches” on page 9-20.)

**DA:** The acronym for *Destination IP Address*. In an IP packet, this is the destination IP address carried in the header, and identifies the destination intended by the packet’s originator. In an extended ACE, this is the second of two IP addresses required by the ACE to determine whether there is a match between a packet and the ACE. See also “SA”.

**Deny:** An ACE configured with this action causes the switch to drop a packet for which there is a match within an applicable ACL.

**Extended ACL:** This type of Access Control List uses layer-3 IP criteria composed of source and destination IP addresses and (optionally) TCP or UDP port criteria to determine whether there is a match with an IP packet. You can apply extended ACLs to either inbound or outbound routed traffic and to any inbound switched or routed traffic with a DA belonging to the switch itself. Extended ACLs require an identification number (ID) in the range of 100 - 199 or an alphanumeric name.

**Implicit Deny:** If the switch finds no matches between a routed packet and the configured criteria in an applicable ACL, then the switch denies (drops) the packet with an implicit “deny IP any” operation. You can preempt the implicit “deny IP any” in a given ACL by configuring `permit IP any` (standard) or `permit IP any any` (extended) as the last explicit ACE in the ACL. Doing so permits any routed packet that is not explicitly permitted or denied by other ACEs configured sequentially earlier in the ACL. Unless otherwise noted, “implicit deny IP any” refers to the “deny” action enforced by both standard and extended ACLs.

**Inbound Traffic:** For the purpose of defining where the switch applies ACLs to filter traffic, inbound traffic is any IP packet that:

- *Enters the switch* on a given subnet.
- Has a destination IP address (DA) that meets either of these criteria:
  - The packet’s DA is for an external device on a different subnet.
  - The packet’s DA is for an IP address configured on the switch itself. (This increases your options for protecting the switch from unauthorized management access.)

Because ACLs are assigned to VLANs, an ACL that filters inbound traffic on a particular VLAN examines packets meeting the above criteria that have entered the switch through any port on that VLAN.
Outbound Traffic: For defining the points where the switch applies ACLs to filter traffic, outbound traffic is routed traffic leaving the switch through a physical port; that is, traffic received on a port in one VLAN (subnet) and sent through a port on another VLAN to another device. This requires that you enable IP routing on the switch. The switch does not apply ACLs internally where routed traffic moves between VLANs. Note that for ACL purposes, “outbound traffic” does not include traffic received on one port and switched to the outbound queue of another port on the same VLAN (subnet); that is, traffic arriving on and leaving the switch on the same VLAN. (Refer also to “ACL Inbound and Outbound Application Points” on page 9-8.)

Permit: An ACE configured with this action allows the switch to forward a routed packet for which there is a match within an applicable ACL.

SA: The acronym for Source IP Address. In an IP packet, this is the source IP address carried in the IP header, and identifies the packet’s sender. In an extended ACE, this is the first of two IP addresses used by the ACE to determine whether there is a match between a packet and the ACE. See also “DA”.

Standard ACL: This type of Access Control List uses layer-3 IP criteria of source IP address to determine whether there is a match with an IP packet. You can apply standard ACLs to either inbound or outbound routed traffic and to any inbound switched or routed traffic with a DA belonging to the switch itself. Standard ACLs require an identification number (ID) in the range of 100 - 199 or an alphanumeric name.

Wildcard: The part of a mask that indicates the bits in a packet’s IP addressing that do not need to match the corresponding bits specified in an ACL. See also ACL Mask on page 9-6.
Overview

Types of IP ACLs

**Standard ACL:** Use a standard ACL when you need to permit or deny traffic based on source IP address only. Standard ACLs are also useful when you need to quickly control a performance problem by limiting traffic from a subnet, group of devices, or a single device. (This can block all IP traffic from the configured source, but does not hamper traffic from other sources within the network.) This ACL type uses a numeric ID of 1 through 99 or an alphanumeric ID string. You can specify a single host, a finite group of hosts, or any host.

**Extended ACL:** Extended ACLs are useful whenever simple IP source address restrictions do not provide the breadth of traffic selection criteria you want to exercise on a VLAN interface. Extended ACLs allow use of the following criteria:

- Source and destination IP addresses
- TCP application criteria
- UDP application criteria

**ACL Inbound and Outbound Application Points**

You can apply ACL filtering to the following types of traffic:

- IP traffic routed between different subnets. (IP routing *must* be enabled.)

- IP traffic carrying a destination address (DA) on the switch itself. In figure 9-1, below, this would be any of the IP addresses shown in VLANs “A”, “B”, and “C” on the switch. (IP routing need not be enabled.)

The switch can apply ACL filtering to traffic *entering or leaving the switch* on VLANs configured to apply ACL filters. (When you assign an ACL to a VLAN, you must specify whether the ACL will filter inbound or outbound traffic. For example, in figure 9-1:
You would assign either an inbound ACL on VLAN “A” or an outbound ACL on VLAN “B” to filter a packet routed between subnets; that is, from the workstation 18.28.10.5 on VLAN “A” to the server at 18.28.20.99 on VLAN “B”. (An outbound ACL on VLAN “A” or an inbound ACL on VLAN “B” would not filter the packet.)

Where multiple subnets are configured on the same VLAN, if:
- Traffic you want to filter moves between subnets on the same VLAN.
- The traffic source and destination IP addresses are on devices external to the switch.

Then you can use either inbound or outbound ACLs to filter the traffic on the VLAN (because the traffic moves between subnets but enters and leaves the switch in the same VLAN.)

ACLs do not filter traffic that remains in the same subnet from source to destination (switched traffic) unless the destination IP address (DA) is on the switch itself.

Features Common to All ACLs
- On any VLAN you can apply one ACL to inbound traffic and one ACL to outbound traffic. You can use the same ACL or different ACLs for the inbound and outbound traffic.
- Any ACL can have multiple entries (ACEs).
Access Control Lists (ACLs)

Overview

- You can apply any one ACL to multiple VLANs.
- A source or destination IP address and a mask, together, can define a single host, a range of hosts, or all hosts.
- The IP address(es) assigned to a VLAN must not be configured from a DHCP server.
- Every standard ACL includes an implied “deny IP any” as the last entry, and every extended ACL includes an implied “deny IP any any” as the last entry. The switch applies this action to any packets that do not match other criteria in the ACL.
- In any ACL, you can apply an ACL log function to ACEs that have a “deny” action. The logging occurs when there is a match on a “deny” ACE. (The switch sends ACL logging output to Syslog and, optionally, to a console session.)

You can configure ACLs using either the CLI or a text editor. The text-editor method is recommended when you plan to create or modify an ACL that has more entries than you can easily enter or edit using the CLI alone. Refer to “Editing ACLs and Creating an ACL Offline” on page 9-53.

General Steps for Planning and Configuring ACLs

1. Identify the traffic type to filter. Options include:
   - Any routed IP traffic
   - Routed TCP traffic only
   - Routed UDP traffic only
2. The SA and/or the DA of routed traffic you want to permit or deny.
3. Determine the best points at which to apply specific ACL controls. For example, you can improve network performance by filtering unwanted traffic at the edge of the network instead of in the core. Also, on the switch itself, you can improve performance by filtering unwanted traffic where it is inbound to the switch instead of outbound.
4. Design the ACLs for the control points you have selected. Where you are using explicit “deny” ACEs, you can optionally use the ACL logging feature to help verify that the switch is denying unwanted packets where intended. Remember that excessive ACL logging activity can degrade the switch's performance. (Refer to “Enable ACL “Deny” Logging” on page 9-59.)
5. Create the ACLs in the selected switches.
6. Assign the ACLs to filter the inbound and/or outbound traffic on static VLAN interfaces configured on the switch.

7. Enable IP routing on the switch. (Except for an ACL configured to filter traffic having the switch itself as the destination IP address, IP routing must be enabled before ACLs will operate.)

8. Test for desired results.

For more details on ACL planning considerations, refer to “Planning an ACL Application” on page 9-16.

---

**Notes on IP Routing**

To activate an ACL to screen inbound traffic for routing between subnets, assign the ACL to the statically configured VLAN on which the traffic enters the switch. Also, ensure that IP routing is enabled. Similarly, to activate an ACL to screen routed, outbound traffic, assign the ACL to the statically configured VLAN on which the traffic exits from the switch. The only exception to these rules is for an ACL configured to screen inbound traffic with a destination IP address on the switch. In this case, an ACL assigned to a VLAN screens traffic addressed to an IP address on the switch, regardless of whether IP routing is also enabled. (ACLs do not screen outbound traffic generated by the switch, itself. Refer to “ACL Screening of Traffic Generated by the Switch” on page 9-63.)

---

**Caution Regarding the Use of Source Routing**

Source routing is enabled by default on the switch and can be used to override ACLs. For this reason, if you are using ACLs to enhance network security, the recommended action is to use the `no ip source-route` command to disable source routing on the switch. (If source routing is disabled in the running-config file, the `show running` command includes “no ip source-route” in the running-config file listing.)
Access Control Lists (ACLs)

ACL Operation

Introduction

An ACL is a list of one or more Access Control Entries (ACEs), where each ACE consists of a matching criteria and an action (permit or deny). An ACL applies only to the switch in which it is configured. ACLs operate on assigned static VLANs, and filter these traffic types:

- Routed traffic entering or leaving the switch on a VLAN. (Note that ACLs do not screen traffic at the internal point where traffic moves between VLANs or subnets within the switch. Refer to “ACL Inbound and Outbound Application Points” on page 9-8.)

- Switched or routed traffic entering the switch on a VLAN and having an IP address on the switch as the destination

You can apply one inbound ACL and one outbound ACL to each static VLAN configured on the switch. The complete range of options per VLAN includes:

- **No ACL** assigned to a static VLAN. (In this case, all traffic entering or leaving the switch on the VLAN does so without any ACL filtering, which is the default.)

- **One ACL** assigned to filter *either* the inbound or the outbound traffic entering or leaving the switch on a static VLAN.

- **One ACL** assigned to filter *both* the inbound and the outbound traffic entering or leaving the switch on a static VLAN.

- **Two different ACLs** assigned to a static VLAN; one for filtering traffic entering the switch and one for filtering traffic leaving the switch.

**Note**

On a given switch, after you assign an ACL to a static VLAN, the default action for all physical ports belonging to the VLAN is to deny any traffic that is not specifically permitted by the ACL. (This applies only in the direction of traffic flow filtered by the ACL.)
The Packet-Filtering Process

Sequential Comparison and Action. When the switch uses an ACL to filter a packet, it sequentially compares each ACE’s filtering criteria to the corresponding data in the packet until it finds a match.

For a packet with a source IP address of 18.28.156.3, the switch:

1. Compares the packet to this ACE first.
2. Since there is not a match with the first ACE, the switch then compares the packet to the second ACE, where there is also not a match.
3. The switch compares the packet to the third ACE. There is a match because the 0.0.0.15 mask includes the source IP address. The switch then denies (drops) the packet.
4. The packet is not compared to the fourth ACE.

Figure 9-2. Example of Sequential Comparison

That is, the switch tries the first ACE in the list. If there is not a match, it tries the second ACE, and so on. When a match is found, the switch invokes the configured action for that entry (permit or drop the packet) and no further comparisons of the packet are made with the remaining ACEs in the ACL. This means that when the switch finds an ACE whose criteria matches a packet, it invokes the action configured for that ACE, and any remaining ACEs in the ACL are ignored. Because of this sequential processing, successfully implementing an ACL depends in part on configuring ACEs in the correct order for the overall policy you want the ACL to enforce.

Implicit Deny. If a packet does not have a match with the criteria in any of the ACEs in the ACL, the switch denies (drops) the packet. (This is termed implicit deny.) If you need to override the implicit deny so that any packet that does not have a match will be permitted, then you can enter permit any as the last ACE in the ACL. This directs the switch to permit (forward) any packets that do not have a match with any earlier ACE listed in the ACL, and prevents these packets from being filtered by the implicit deny.
For ACLs configured to filter inbound packets on a VLAN, remember that Implicit Deny filters routed packets and any bridged packets with a DA specifying the switch itself. This operation helps to prevent management access from unauthorized IP sources.

1. If a match is not found with the first ACE in an ACL, the switch proceeds to the next ACE and so on.
2. If a match with an explicit ACE is subsequently found, the packet is either permitted (forwarded) or denied (dropped), depending on the action specified in the matching ACE. In this case the switch ignores all subsequent ACEs in the ACL.
3. If a match is not found with any explicit ACE in the ACL, the switch invokes the implicit deny IP any at the end of every ACL, and drops the packet.

**Note:** If the list includes a permit IP any entry, no packets can reach the implicit deny IP any at the end of the list. Also, a permit IP any ACE at any point in an ACL defeats the purpose of any subsequent ACEs in the list.

Figure 9-3. The Packet-Filtering Process in an ACL with N Entries (ACEs)
The order in which an ACE occurs in an ACL is significant. For example, if an ACL contains six ACEs, but the first ACE is a “permit IP any”, then the ACL permits all IP traffic, and the remaining ACEs in the list do not apply, even if they specify criteria that would make a match with any of the traffic permitted by the first ACE.

For example, suppose you want to configure an ACL on the switch (with an ID of “100”) to invoke these policies:

1. Permit all inbound traffic on VLAN 12 routed from IP address 11.11.11.42.
2. Deny only the inbound Telnet traffic routed from address 11.11.11.101.
3. Permit only inbound Telnet traffic routed from IP address 11.11.11.33.
4. Deny all other inbound routed traffic on VLAN 12.

The following ACL model, when assigned to inbound filtering on VLAN 12, supports the above case:

```
HPswitch(config)# show access-list config
ip access-list extended "100"
   1 permit ip 11.11.11.42 0.0.0.0 0.0.0.0 255.255.255.255
   2 deny tcp 11.11.11.101 0.0.0.0 0.0.0.0 255.255.255.255 eq 23
   3 permit ip 11.11.11.101 0.0.0.0 0.0.0.0 255.255.255.255
   4 permit tcp 11.11.11.33 0.0.0.0 0.0.0.0 255.255.255.255 eq 23
   5 <implicit deny IP any>
```

HPswitch(config)# vlan 12 ip access-group 100 in

---

**Figure 9-4. Example of How an ACL Filters Packets**

1. **Permits** IP traffic routed from source address 11.11.11.42. Packets matching this criterion are permitted and will not be compared to any later ACE in the list. Packets not matching this criterion will be compared to the next entry in the list.

2. **Denies** Telnet traffic routed from source address 11.11.11.101. Packets matching this criterion are dropped and are not compared to later criteria in the list. Packets not matching this criterion are compared to the next entry in the list.

3. **Permits** any IP traffic routed from source address 11.11.11.101. Any packets matching this criterion will be permitted and will not be compared to any later criteria in the list. Because this entry comes after the entry blocking Telnet traffic from this same address, there will not be any Telnet packets to compare with this entry; they have already been dropped as a result of matching the preceding entry.

4. **Permits** Telnet traffic routed from source address 11.11.11.33. Packets matching this criterion are permitted and are not compared to any later criteria in the list. Packets not matching this criterion are compared to the next entry in the list.

5. This entry does not appear in an actual ACL, but is implicit as the last entry in every ACL. Any routed packets that do not match any of the criteria in the ACL's preceding entries will be denied (dropped), and will not cross VLAN 12.
Access Control Lists (ACLs)
Planning an ACL Application

It is important to remember that this ACL (and all ACLs) include an implicit “deny IP any”. That is, routed IP packets (and switched packets having the switch as the destination IP address) that the ACL does not explicitly permit or deny will be implicitly denied, and therefore dropped instead of forwarded on the VLAN. You can preempt the implicit deny by inserting a “permit IP any” at the end of an ACL, but this solution does not apply in the preceding example, where the intention is for the switch to forward only explicitly permitted packets routed on VLAN 12.

**Overriding the Implicit “deny IP any”**. If you want an ACL to permit any routed packets that are not explicitly denied by other entries in the ACL, you can do so by configuring a **permit any** entry as the last entry in the ACL. Doing so permits any packet not explicitly denied by earlier entries.

---

**Planning an ACL Application**

Before creating and implementing ACLs, you need to define the policies you want your ACLs to enforce, and understand how your ACLs will impact your network users.

**Traffic Management and Improved Network Performance**

You can use ACLs to block unnecessary traffic caused by individual hosts, workgroups, or subnets, and to block user access to subnets, devices, and services. Answering the following questions can help you to design and properly position ACLs for optimum network usage.

- What are the logical points for minimizing unwanted traffic? In many cases it makes sense to prevent unwanted traffic from reaching the core of your network by configuring ACLs to drop unwanted traffic at or close to the edge of the network. (The earlier in the network path you can block unwanted traffic, the greater the benefit for network performance.)

- What traffic should you explicitly block? Depending on your network size and the access requirements of individual hosts, this can involve creating a large number of ACEs in a given ACL (or a large number of ACLs), which increases the complexity of your solution.
What traffic can you implicitly block by taking advantage of the implicit **deny IP any** to deny traffic that you have not explicitly permitted? This can reduce the number of entries needed in an ACL.

What traffic should you permit? In some cases you will need to explicitly identify permitted traffic. In other cases, depending on your policies, you can insert a **permit any** entry at the end of an ACL. This means that all IP traffic not specifically matched by earlier entries in the list will be permitted.

**Security**

ACLs can enhance security by blocking routed IP traffic carrying an unauthorized source IP address (SA). This can include:

- Blocking access to or from subnets in your network
- Blocking access to or from the internet
- Blocking access to sensitive data storage or restricted equipment
- Preventing the use of specific TCP or UDP functions (such as Telnet, SSH, web browser) for unauthorized access

You can also enhance switch management security by using ACLs to block bridged IP traffic that has the switch itself as the destination address (DA).

---

**Caution**

ACLs can enhance network security by blocking selected IP traffic, and can serve as one aspect of maintaining network security. *However, because ACLs do not provide user or device authentication, or protection from malicious manipulation of data carried in IP packet transmissions, they should not be relied upon for a complete security solution.*

---

**Note**

ACLs in the Series 5300XL switches do not screen non-IP traffic such as AppleTalk and IPX.
Guidelines for Planning the Structure of an ACL

The first step in planning a specific ACL is to determine where you will apply it. (Refer to “ACL Inbound and Outbound Application Points” on page 9-8.) You must then determine the order in which you want the individual ACEs in the ACL to filter traffic.

- The first match dictates the action on a packet. Subsequent matches are ignored.
- On any ACL, the switch implicitly denies packets that are not explicitly permitted or denied by the ACEs configured in the ACL. If you want the switch to forward a packet for which there is not a match in an ACL, add the “permit IP any” function as the last ACE in an ACL. This ensures that no packets reach the implicit “deny IP any” case.
- Generally, you should list ACEs from the most specific (individual hosts) to the most general (subnets or groups of subnets) unless doing so permits traffic that you want dropped. For example, an ACE allowing a small group of workstations to use a specialized printer should occur earlier in an ACL than an entry used to block widespread access to the same printer.

ACL Configuration and Operating Rules

- **Routing.** Except for any IP traffic with a DA on the switch itself, ACLs filter only routed traffic. Thus, if routing is not enabled on the switch, there is no routed traffic for ACLs to filter. (To enable routing, execute `ip routing` at the global configuration level.) For more on routing, refer to the chapter titled “IP Routing Features” in this manual.

- **Per-Switch ACL Limits.** At a minimum an ACL must have one, explicit “permit” or “deny” Access Control Entry. You can configure up to 255 ACL assignments to VLANs, as follows:
  - Standard ACLs: Up to 99; numeric range: 1 - 99
  - Extended ACLs: Up to 100; numeric range: 100 - 199
  - Named (Extended or Standard) ACLs: Up to 255 (minus any numeric ACL assignments)
  - Total ACEs in all ACLs: 1024

- **Implicit “deny any”**: In any ACL, the switch automatically applies an implicit “deny IP any” that does not appear in `show` listings. This means that the ACL denies any packet it encounters that does not have a match with an entry in the ACL. Thus, if you want an ACL to
permit any packets that you have not expressly denied, you must enter a **permit any** or **permit ip any any** as the last ACE in an ACL. Because, for a given packet the switch sequentially applies the ACEs in an ACL until it finds a match, any packet that reaches the **permit any** or **permit ip any any** entry will be permitted, and will not encounter the “deny ip any” ACE the switch automatically includes at the end of the ACL. For an example, refer to figure 9-4 on page 9-15.

- **Explicitly Permitting Any IP Traffic:** Entering a **permit any** or a **permit ip any any** ACE in an ACL permits all IP traffic not previously permitted or denied by that ACL. Any ACEs listed after that point do not have any effect.

- **Explicitly Denying Any IP Traffic:** Entering a **deny any** or a **deny ip any any** ACE in an ACL denies all IP traffic not previously permitted or denied by that ACL. Any ACEs listed after that point have no effect.

- **Replacing One ACL with Another:** The last ACL assigned for inbound (“in”) or outbound (“out”) packet filtering on an interface replaces any other ACL previously configured for the same purpose. For example, if you configured ACL 100 to filter inbound traffic on VLAN 20, but later, you configured ACL 112 to filter inbound traffic on this same VLAN, ACL 112 replaces ACL 100 as the ACL to use for filtering inbound traffic on VLAN 20.

- **ACLs Operate On Static VLANs:** You can assign an ACL to any VLAN that is statically configured on the switch. ACLs do not operate with dynamic VLANs.

- **An ACL Affects All Physical Ports in a Static VLAN:** An ACL assigned to a VLAN applies to all physical ports on the switch that belong to that VLAN, including ports that have dynamically joined the VLAN.

- **ACLs Screen Traffic Entering or Leaving the Switch on a VLAN:** On a given VLAN, ACLs can screen inbound or outbound traffic at the point where it enters or leaves the switch. ACLs do not screen traffic moving between VLANs within the switch or between subnets in a multinetted VLAN. (See figure 9-1.)

- **ACLs Do Not Filter Switched Traffic Unless the Switch Itself is the DA:** ACLs do not filter:
  - Traffic moving between ports belonging to the same subnet
  - Traffic leaving the switch with an SA on the switch itself

ACLs *do* filter switched or routed traffic having a DA on the switch.
How an ACE Uses a Mask To Screen Packets for Matches

When the switch applies an ACL to inbound or outbound traffic in a VLAN, each ACE in the ACL uses an IP address and ACL mask to enforce a selection policy on the packets being screened. That is, the mask determines the range of IP addresses (SA only or SA/DA) that constitute a match between the policy and a packet being screened.

What Is the Difference Between Network (or Subnet) Masks and the Masks Used with ACLs?

In common IP addressing, a network (or subnet) mask defines which part of the IP address to use for the network number and which part to use for the hosts on the network. For example:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
<th>Network Address</th>
<th>Host Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.38.252.195</td>
<td>255.255.255.0</td>
<td>first three octets</td>
<td>The fourth octet.</td>
</tr>
<tr>
<td>18.38.252.195</td>
<td>255.255.248.0</td>
<td>first two octets and the left-most five bits of the third octet</td>
<td>The right most three bits of the third octet and all bits in the fourth octet.</td>
</tr>
</tbody>
</table>

Thus, the bits set to 1 in a network mask define the part of an IP address to use for the network number, and the bits set to 0 in the mask define the part of the address to use for the host number.

In an ACL, IP addresses and masks provide the criteria for determining whether to deny or permit a packet, or to pass it to the next ACE in the list. If there is a match, the deny or permit action occurs. If there is not a match, the packet is compared with the next ACE in the ACL. Thus, where a standard network mask defines how to identify the network and host numbers in an IP address, the mask used with ACEs defines which bits in a packet’s IP address must match the corresponding bits in the IP address listed in an ACE, and which bits can be wildcards.
Rules for Defining a Match Between a Packet and an Access Control Entry (ACE)

- For a given ACE, when the switch compares an IP address and corresponding mask in the ACE to an IP address carried in a packet:
  - **A mask-bit setting of 0 (“off”)** requires that the corresponding bit in the packet’s IP address and in the ACE’s IP address must be the same. That is, if a bit in the ACE’s IP address is set to 1 (“on”), the same bit in the packet’s IP address must also be 1.
  - **A mask-bit setting of 1 (“on”)** means the corresponding bit in the packet’s IP address and in the ACE’s IP address do not have to be the same. That is, if a bit in the ACE’s IP address is set to 1, the same bit in the packet’s IP address can be either 1 or 0 (“on” or “off”).

For an example, refer to “Example of How the Mask Bit Settings Define a Match” on page 9-23.

- In any ACE, a mask of all ones means *any* IP address is a match. Conversely, a mask of all zeros means the *only* match is an IP address identical to the host IP address specified in the ACL.

- Depending on your network, a single ACE that allows a match with more than one source or destination IP address may allow a match with multiple subnets. For example, in a network with a prefix of 31.30.240 and a subnet mask of 255.255.240.0 (the left most 20 bits), applying an ACL mask of 0.0.31.255 causes the subnet mask and the ACL mask to overlap one bit, which allows matches with hosts in two subnets: 31.30.224.0 and 31.30.240.0.

<table>
<thead>
<tr>
<th>Bit Position in the Third Octet of Subnet Mask 255.255.240.0</th>
<th>128</th>
<th>64</th>
<th>32</th>
<th>16</th>
<th>8</th>
<th>4</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet Mask Bits</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Mask Bit Settings Affecting Subnet Addresses</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1 or 0</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

This ACL supernetting technique can help to reduce the number of ACLs you need. You can apply it to a multinetted VLAN and to multiple VLANs. However, ensure that you exclude subnets that do not belong in the policy. If this creates a problem for your network, you can eliminate the unwanted match by making the ACEs in your ACL as specific as possible, and using multiple ACEs carefully ordered to eliminate unwanted matches.
Every IP address and mask pair (source or destination) used in an ACE creates one of the following policies:

- **Any IP address fits the matching criteria.** In this case, the switch automatically enters the IP address and mask in the ACE. For example:

  access-list 1 deny any

produces this policy in an ACL listing:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
</tr>
</tbody>
</table>

This policy states that every bit in every octet of a packet’s SA is a wildcard, which covers any IP address.

- **One IP address fits the matching criteria.** In this case, you provide the IP address and the switch provides the mask. For example:

  access-list 1 permit host 18.28.100.15

produces this policy in an ACL listing:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.28.100.15</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

This policy states that every bit in every octet of a packet’s SA must be the same as the corresponding bit in the SA defined in the ACE.

- **A group of IP addresses fits the matching criteria.** In this case you provide both the IP address and the mask. For example:

  access-list 1 permit 18.28.32.1 0.0.0.31

produces this policy in an ACL listing:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.28.32.1</td>
<td>0.0.0.31</td>
</tr>
</tbody>
</table>

This policy states that:

- In the first three octets of a packet’s SA, every bit must be set the same as the corresponding bit in the SA defined in the ACE.
- In the last octet of a packet’s SA, the first three bits must be the same as in the ACE, but the last five bits are wildcards and can be any value.

Unlike subnet masks, the wildcard bits in an ACL mask need not be contiguous. For example, 0.0.7.31 is a valid ACL mask. However, a subnet mask of 255.255.248.224 is not a valid subnet mask.
Example of How the Mask Bit Settings Define a Match. Assume an ACE where the second octet of the mask for an SA is 7 (the rightmost three bits are “on”, or “1”) and the second octet of the corresponding SA in the ACE is 31 (the rightmost five bits). In this case, a match occurs when the second octet of the SA in a packet being filtered has a value in the range of 24 to 31. Refer to table 9-2, below.

Table 9-2. Example of How the Mask Defines a Match

<table>
<thead>
<tr>
<th>Location of Octet</th>
<th>Bit Position in the Octet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>128</td>
</tr>
<tr>
<td>SA in ACE</td>
<td>0</td>
</tr>
<tr>
<td>Mask for SA</td>
<td>0</td>
</tr>
<tr>
<td>Corresponding Octet of a Packet's SA</td>
<td>0</td>
</tr>
</tbody>
</table>

The shaded area indicates bits in the packet that must exactly match the bits in the source IP in the ACE. Wherever the mask bits are ones (wildcards), the IP bits in the packet can be any value, and where the mask bits are zeros, the IP bits in the packet must be the same as the IP bits in the ACE. Note: This example covers only one octet of an IP address. An actual ACE applies this method to all four octets of an IP address.

Example of Allowing Only One IP Address (“Host” Option). Suppose, for example, that you have configured the ACL in figure 9-5 to filter inbound packets on VLAN 20. Because the mask is all zeros, the ACE policy dictates that a match occurs only when the source IP address on such packets is identical to the IP address configured in the ACE.

This ACL (a standard ACL named “Fileserver”) includes an ACE (Access Control Entry) that permits matches only with the packets received from IP address 18.28.252.117 (the SA). Packets from any other source do not match and are denied.

Inbound Packet “A” On VLAN 20
- Destination Address: 18.35.248.184
- Source Address: 18.28.252.117

Inbound Packet “B” On VLAN 20
- Destination Address: 18.35.248.184
- Source Address: 18.28.252.120

The VLAN permits packet “A” because its source IP address matches the source address in the ACE.

The VLAN denies packet “B” because its source IP address does not match the source address in the ACE.
Examples Allowing Multiple IP Addresses. Table 9-3 provides examples of how to apply masks to meet various filtering requirements.

<table>
<thead>
<tr>
<th>IP Address in the ACE</th>
<th>Mask</th>
<th>Policy for a Match Between a Packet and the ACE</th>
<th>Allowed IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A: 18.38.252.195</td>
<td>0.0.0.255</td>
<td>Exact match in first three octets only.</td>
<td>18.38.252.&lt; 0-255 &gt;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(See row A in table 9-4, below.)</td>
<td></td>
</tr>
<tr>
<td>B: 18.38.252.195</td>
<td>0.0.7.255</td>
<td>Exact match in the first two octets and the leftmost five bits (248) of the third octet.</td>
<td>18.38.&lt; 248-255 &gt;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(In the third octet, only the rightmost three bits are wildcard bits. The leftmost five bits must be a match, and in the ACE, these bits are all set to 1. See row B in table 9-4, below.)</td>
<td></td>
</tr>
<tr>
<td>C: 18.38.252.195</td>
<td>0.0.0.0</td>
<td>Exact match in all octets.</td>
<td>18.38.252.195</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(There are no wildcard bits in any of the octets. See row C in table 9-4, below.)</td>
<td></td>
</tr>
<tr>
<td>D: 18.38.252.195</td>
<td>0.15.255.255</td>
<td>Exact match in the first octet and the leftmost four bits of the second octet.</td>
<td>18.&lt; 32-47 &gt;.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(In the second octet, the rightmost four bits are wildcard bits. See row D in table 9-4, below.)</td>
<td></td>
</tr>
</tbody>
</table>

<p>| Table 9-4. Mask Effect on Selected Octets of the IP Addresses in Table 9-3 |
|-----------------------------|-----------------|-----------------|--------|--------|--------|--------|--------|--------|--------|</p>
<table>
<thead>
<tr>
<th>IP Addr</th>
<th>Octet</th>
<th>Mask</th>
<th>Octet Range</th>
<th>128</th>
<th>64</th>
<th>32</th>
<th>16</th>
<th>8</th>
<th>4</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>3</td>
<td>0</td>
<td>252</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all bits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>B</td>
<td>3</td>
<td>7</td>
<td>248-255</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>last 3 bits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>4</td>
<td>0</td>
<td>195</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all bits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td>2</td>
<td>15</td>
<td>32-47</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>last 4 bits</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Shaded areas indicate bit settings that must be an exact match.

If there is a match between the policy in the ACE and the IP address in a packet, then the packet is either permitted or denied, according to how the ACE is configured. If there is not a match, the next ACE in the ACL is then applied to the packet. The same operation applies to a destination IP address (DA) used in an extended ACE. (Where an ACE includes both source and destination IP addresses, there is one IP-address/ACL-mask pair for the source address, and another IP-address/ACL-mask pair for the destination address. See “Configuring and Assigning an ACL” on page 9-25.)

CIDR Notation. For information on using CIDR notation to specify ACL masks, refer to “Using CIDR Notation To Enter the ACL Mask” on page 9-32.
Configuring and Assigning an ACL

<table>
<thead>
<tr>
<th>ACL Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring and Assigning a Numbered, Standard ACL</td>
<td>9-33</td>
</tr>
<tr>
<td>Configuring and Assigning a Numbered, Extended ACL</td>
<td>9-38</td>
</tr>
<tr>
<td>Configuring a Named ACL</td>
<td>9-44</td>
</tr>
<tr>
<td>Enabling or Disabling ACL Filtering</td>
<td>9-46</td>
</tr>
</tbody>
</table>

Overview

General Steps for Implementing ACLs

1. Configure at least one ACL. This creates and stores the ACL(s) in the switch configuration.

2. Assign an ACL. This applies the ACL to either the inbound or outbound traffic on a designated VLAN.

3. Enable IP routing. Except for instances where the switch is the destination, assigned ACLs screen IP traffic only when routing is enabled on the switch.

Caution Regarding the Use of Source Routing

Source routing is enabled by default on the switch and can be used to override ACLs. For this reason, if you are using ACLs to enhance network security, the recommended action is to disable source routing on the switch. To do so, execute `no ip source-route`. 
Types of ACLs

- **Standard ACL:** Uses only a packet’s source IP address as a criterion for permitting or denying the packet. For a standard ACL ID, use either a unique numeric string in the range of 1-99 or a unique name string of up to 64 alphanumeric characters.

- **Extended ACL:** Offers the following criteria as options for permitting or denying a packet:
  - Source IP address
  - Destination IP address
  - TCP or UDP criteria

  For an extended ACL ID, use either a unique number in the range of 100-199 or a unique name string of up to 64 alphanumeric characters.

You should carefully plan your ACL application before configuring specific ACLs. For more on this topic, refer to “Planning an ACL Application” on page 9-16.

ACL Configuration Structure

After you enter an ACL command, you may want to inspect the resulting configuration. This is especially true where you are entering multiple ACEs into an ACL. Also, it will be helpful to understand the configuration structure when using later sections in this chapter.

The basic ACL structure includes three elements:

1. List type and name: This identifies the ACL as **standard** or **extended** and shows the ACL name.

2. One or more deny/permit list entries (ACEs): One entry per line.

<table>
<thead>
<tr>
<th>Element</th>
<th>Stnd</th>
<th>Ext</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID Range</td>
<td>1 - 99</td>
<td>100 - 199</td>
<td>You can also use an alphanumeric name of up to 64 characters, including spaces.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Minimum ACEs per ACL</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum ACEs Per ACL and per Switch</td>
<td>1024</td>
</tr>
</tbody>
</table>

3. Implicit **deny any:** Where an ACL is in use, the switch denies any packets that do not have a match with the ACEs explicitly configured in the ACL. The implicit **deny any** does not appear in ACL configuration listings, but
always functions when the switch uses an ACL to filter packets. (You cannot delete the implicit “deny any”, but you can supersede it with a “permit any” statement.)

Standard ACL Structure

Individual ACEs in a standard ACL include only a permit/deny “type” statement, the source IP addressing, and an optional log command (available with “deny” statements).

```
ip access-list < type > "< id-string >"  
   permit host < source-ip-address >  
   deny < source-ip-address > < acl-mask > [log]  
   .  
   .  
   permit any  
   exit
```

Figure 9-6. Example of the General Structure for a Standard ACL

For example, figure 9-7 shows how to interpret the entries in a standard ACL.
Extended ACL Configuration Structure

Individual ACEs in an extended ACL include:

- A permit/deny “type” statement
- Source IP addressing
- Optional TCP or UDP port type with optional source port ID and operator and/or optional destination port ID and operator
- Destination IP addressing
- Optional ACL \texttt{log} command

\[
\text{ip access-list } < \text{type}>" < \text{id-string}>" < \text{permit | deny}> ip
\begin{align*}
< \text{source-ip-address}> < \text{source-acl-mask}> \\
< \text{destination-ip-address}> < \text{destination-acl-mask}> [\text{log}]
\end{align*}
\]
\[
< \text{permit | deny}> tcp
\begin{align*}
< \text{source-ip-address}> < \text{source-acl-mask}> [< \text{operator}> < \text{port-id}>] \\
< \text{destination-ip-address}> < \text{destination-acl-mask}> [< \text{operator}> < \text{port-id}>] [\text{log}]
\end{align*}
\]
\[
< \text{permit | deny}> udp
\begin{align*}
< \text{source-ip-address}> < \text{source-acl-mask}> [< \text{operator}> < \text{port-id}>] \\
< \text{destination-ip-address}> < \text{destination-acl-mask}> [< \text{operator}> < \text{port-id}>] [\text{log}]
\end{align*}
\]

Note: The optional log function appears only with “deny” aces.

\textbf{Figure 9-8. General Structure for an Extended ACL}
For example, figure 9-9 shows how to interpret the entries in an extended ACL.

<table>
<thead>
<tr>
<th>Protocol Types</th>
<th>ACL List Heading with List Type and ID String (Name or Number)</th>
<th>Specifies all destination IP addresses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Address and Mask. Upper entry denies certain UDP packets from a single host. Lower entry denies all UDP packets from all hosts.</td>
<td>Optional Source UDP or TCP Operator and Port Number In this case, the ACL specifies UDP port 69 packets coming from the source IP address.</td>
<td>Denies TCP Port 80 traffic to any destination from any source.</td>
</tr>
<tr>
<td>Optional Destination UDP or TCP Operator and Range of Port Numbers In this case, the ACL specifies UDP port numbers 3680-3690.</td>
<td>Destination IP Address and Mask</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 9-9. Example of a Displayed Extended ACL Configuration**

### ACL Configuration Factors

#### The Sequence of Entries in an ACL Is Significant

When the switch uses an ACL to determine whether to permit or deny a packet on a particular VLAN, it compares the packet to the criteria specified in the individual Access Control Entries (ACEs) in the ACL, beginning with the first ACE in the list and proceeding sequentially until a match is found. When a match is found, the switch applies the indicated action (permit or deny) to the packet. This is significant because, once a match is found for a packet, subsequent ACEs in the same ACL will not be used for that packet, regardless of whether they match the packet.

For example, suppose that you have applied the ACL shown in figure 9-10 to inbound traffic on VLAN 1 (the default VLAN):
Access Control Lists (ACLs)
Configuring and Assigning an ACL

```
ip access-list extended "101"
  deny ip 18.28.235.10 0.0.0.0 0.0.0.0 255.255.255.255
  deny ip 18.28.245.89 0.0.0.0 0.0.0.0 255.255.255.255
  permit tcp 18.28.18.100 0.0.0.0 18.28.237.1 0.0.0.0
  deny tcp 18.28.18.100 0.0.0.0 0.0.0.0 255.255.255.255
  permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
```

Figure 9-10. Example of a Standard ACL that Permits All Traffic Not Implicitly Denied

Table 9-5. Effect of the Above ACL on Inbound Traffic in the Assigned VLAN

<table>
<thead>
<tr>
<th>Line #</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Shows list type (extended) and ID (101).</td>
</tr>
<tr>
<td>2</td>
<td>A packet from IP source address 18.28.235.10 will be denied (dropped). This line filters out all packets received from 18.28.235.10. As a result, IP traffic from that device will not be routed and packets from that device will not be compared against any later entries in the list.</td>
</tr>
<tr>
<td>3</td>
<td>A packet from IP source 18.28.245.89 will be denied (dropped). This line filters out all packets received from 18.28.245.89. As the result, IP traffic from that device will not be routed and packets from that device will not be compared against any later entries in the list.</td>
</tr>
<tr>
<td>4</td>
<td>A packet from TCP source address 18.28.18.100 with a destination address of 18.28.237.1 will be permitted (forwarded). Since no earlier lines in the list have filtered TCP packets from 18.28.18.100 and destined for 18.28.237.1, the switch will use this line to evaluate such packets. Any packets that meet this criteria will be forwarded. (Any packets that do not meet this TCP source-destination criteria are not affected by this line.)</td>
</tr>
<tr>
<td>5</td>
<td>A packet from TCP source address 18.28.18.100 to any destination address will be denied (dropped). Since, in this example, the intent is to block TCP traffic from 18.28.18.100 to any destination except the destination stated in line 4, this line must follow line 4. (If their relative positions were exchanged, all TCP traffic from 18.28.18.100 would be dropped, including the traffic for the 18.28.18.1 destination.)</td>
</tr>
<tr>
<td>6</td>
<td>Any packet from any IP source address to any destination address will be permitted (forwarded). The only traffic to reach this line will be IP packets not specifically permitted or denied in the earlier lines.</td>
</tr>
<tr>
<td>n/a</td>
<td>The “implicit deny any any” is a function automatically added as the last action in all ACLs. It denies (drops) any IP traffic from any source to any destination that has not found a match with earlier entries in the list. In this example, line 6 permits (forwards) any IP traffic not already permitted or denied by the earlier entries in the list, so there is no traffic remaining for action by the “implicit deny any any” function.</td>
</tr>
<tr>
<td>7</td>
<td>Indicates the end of the ACL.</td>
</tr>
</tbody>
</table>
In Any ACL, There Will Always Be a Match

As indicated in figure 9-10, the switch automatically uses an implicit “deny IP any” (Standard ACL) or “deny IP any any” (Extended ACL) as the last ACE in any ACL. This means that if you configure the switch to use an ACL for filtering either inbound or outbound traffic on a VLAN, any packets not specifically permitted or denied by the explicit entries you create will be denied by the implicit “deny” action. Note that if you want to preempt the implicit “deny” action, insert an explicit \texttt{permit any} or \texttt{permit ip any any} as the last line of the ACL.

A Configured ACL Has No Effect Until You Apply It to an Interface

The switch stores ACLs in the configuration file. Thus, until you actually assign an ACL to a VLAN interface, it is present in the configuration, but not used.

You Can Assign an ACL Name or Number to a VLAN Even if the ACL Does Not Yet Exist in the Switch’s Configuration

In this case, if you subsequently create an ACL with that name or number, the switch automatically applies each ACE as soon as you enter it in the running-config file. Similarly, if you modify an existing ACE in an ACL you already applied to a VLAN, the switch automatically implements the new ACE as soon as you enter it. (See “General ACL Operating Notes” on page 9-63.) The switch allows a maximum of 255 ACLs in any combination of numeric and alphanumeric names, and determines the total from the number of unique ACL names in the configuration. For example, if you configure two ACLs, but assign only one of them to a VLAN, the ACL total is two, for the two unique ACL names. If you then assign the name of a nonexistent ACL to a VLAN, the new ACL total is three, because the switch now has three unique ACL names in its configuration.

Using the CLI To Create an ACL

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list (standard ACLs)</td>
<td>9-33</td>
</tr>
<tr>
<td>access-list (extended ACLs)</td>
<td>9-38</td>
</tr>
<tr>
<td>ip access-list (named ACLs)</td>
<td>9-44</td>
</tr>
</tbody>
</table>
Use either the switch CLI or an offline text editor to create an ACL. This section describes the CLI method, which is recommended for creating short ACLs. (To use the offline method, refer to “Editing ACLs and Creating an ACL Offline” on page 9-53.)

General ACE Rules

These rules apply to all ACEs you create or edit using the CLI:

- ACEs are placed in an ACL according to the sequence in which you enter them (last entered, last listed).
- You can use the CLI to delete an ACE from anywhere in a given ACL by using the “no” form of the command to enter that ACE. However, when you use the CLI to add an ACE, the new entry is always placed at the end of the ACL.
- Duplicate ACEs are allowed in an ACL. However, multiple instances of an ACE have no effect on filtering because the first instance preempts any subsequent duplicates.

For more information, refer to “Editing ACLs and Creating an ACL Offline” on page 9-53.

Using CIDR Notation To Enter the ACL Mask

You can use CIDR (Classless Inter-Domain Routing) notation to enter ACL masks. The switch interprets the bits specified with CIDR notation as the IP address bits in an ACL and the corresponding IP address bits in a packet. The switch then converts the mask to inverse notation for ACL use.

Table 9-6. Examples of CIDR Notation for Masks

<table>
<thead>
<tr>
<th>IP Address Used In an ACL with CIDR Notation</th>
<th>Resulting ACL Mask</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.38.240.125/15</td>
<td>0.1.255.255</td>
<td>The leftmost 15 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/20</td>
<td>0.0.15.255</td>
<td>The leftmost 20 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/21</td>
<td>0.0.7.255</td>
<td>The leftmost 21 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/24</td>
<td>0.0.0.255</td>
<td>The leftmost 24 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/32</td>
<td>0.0.0.0</td>
<td>All bits must match.</td>
</tr>
</tbody>
</table>
Configuring and Assigning a Numbered, Standard ACL

This section describes how to configure numbered, standard ACLs.

- To configure named ACLs, refer to “Configuring a Named ACL” on page 9-44.
- To configure extended, numbered ACLs, refer to “Configuring and Assigning a Numbered, Extended ACL” on page 9-38.

A standard ACL uses only source IP addresses in its ACEs. This type of ACE is useful when you need to:

- Permit or deny traffic based on source IP address only.
- Quickly control the IP traffic from a specific address. This allows you to isolate traffic problems generated by a specific device, group of contiguous devices, or a subnet threatening to degrade network performance. This gives you an opportunity to troubleshoot without sacrificing performance for users outside of the problem area.

You can configure up to 255 standard ACL assignments, depending on how many extended ACL assignments are already configured. (The switch allows a maximum of 255 unique ACL identities; standard and extended combined.) You can identify each standard ACL with a number in the range of 1 - 99, or an alphanumeric string of up to 64 characters. The CLI command process for using an alphanumerical string to name an ACL differs from the command process for a numeric name. For a description of naming an ACL with an alphanumerical character string, refer to “Configuring a Named ACL” on page 9-44. To view the command differences, refer to table 9-1, “Comprehensive Command Summary” on page 9-4.

Note

**Syntax:**  [no] access-list

Creates an ACE in the specified (1-99) access list and indicates the action (deny or permit) to take on a packet if there is a match between the packet and the criterion in the entry. If the ACL does not already exist, this command creates the specified ACL and its first ACE. To create a named ACL, refer to “Configuring a Named ACL” on page 9-44.

< 1-99 >

Specifies the ACL ID number. The switch interprets an ACL with a value in this range as a standard ACL.

**Note:** To create an access list with an alphanumeric name (name-str) instead of a number, refer to “Configuring a Named ACL” on page 9-44.

< deny | permit >

Specifies whether to deny (drop) or permit (forward) a packet that matches the ACE criteria.

< any | host < src-ip-addr > | ip-addr | mask-length >

- **any** — Performs the specified action on any IP packet. Use this criterion to designate packets from any IP address.
- **host** < host ip-address > — Performs the specified action on any IP packet having the < host ip-address > as the source. Use this criterion to designate packets from a single IP address.
- **ip-addr | mask-length** — Performs the specified action on any IP packet having a source address within the range defined by either

  < src-ip-addr / cidr-mask-bits >

  or

  < src-ip-addr < mask >>

Use this criterion to filter packets received from either a subnet or a group of IP addresses. The mask can be in either dotted-decimal format or CIDR format with the number of significant bits. Refer to “Using CIDR Notation To Enter the ACL Mask” on page 9-32.
The mask is applied to the IP address in the ACL to define which bits in a packet’s source IP address must exactly match the IP address configured in the ACL and which bits need not match. Note that specifying a group of contiguous IP addresses may require more than one ACE. For more on how masks operate in ACLs, refer to “How an ACE Uses a Mask To Screen Packets for Matches” on page 9-20.

[log]

Optionally generates an ACL log message if:

• The action is deny.
• There is a match.
• ACL logging is enabled on the switch. (Refer to “Enable ACL “Deny” Logging” on page 9-59.)

(Use the debug command to direct ACL logging output to the current console session and/or to a Syslog server. Note that you must also use the logging < ip-addr > command to specify the IP addresses of Syslog servers to which you want log messages sent. See also “Enable ACL “Deny” Logging” on page 9-59.)

Syntax:  vlan < vid > ip access-group < ASCII-STR > < in | out >

Assigns an ACL, designated by an ACL ID (< ASCII-STR >), to a VLAN.

Example of a Standard ACL. Suppose you wanted to configure a standard ACL and assign it to filter inbound traffic on VLAN 10 in a particular switch:

■ The ID you selected for this ACL is “50”.

■ You want the ACL to deny IP traffic from all hosts except these three:
  • 18.128.100.10
  • 18.128.100.27
  • 18.128.100.14
Access Control Lists (ACLs)
Configuring and Assigning an ACL

- Permits IP traffic from the indicated IP address. Since, for this example, ACL 50 is a new list, this command also creates the ACL.
- Permits IP traffic from the indicated IP address.
- The deny any that the switch implicitly includes in all standard ACLs denies IP packets from IP sources not included in the above three commands.

ACL "50" is listed in the switch configuration.
ACL "50" is assigned to filter inbound traffic on VLAN 10.

Show config lists any ACLs and ACL assignments configured in the startup-config.

Note: To enable traffic filtering with an ACL assigned to a VLAN such as the one shown in this example, IP routing must be enabled on the switch. Otherwise, no ACL filtering occurs.

Figure 9-11. Example of Configuring a Standard ACL To Permit Only Traffic from Specific IP Addresses

In a situation opposite to the above, suppose that you wanted to deny inbound IP traffic received on VLAN 20 from 18.128.93.17 and 18.130.93.25, but permit all other IP traffic on this VLAN. The next ACL achieves this:

```
HPswitch(config)# access-list 50 permit host 18.128.100.10
HPswitch(config)# access-list 50 permit host 18.128.100.27
HPswitch(config)# access-list 50 permit host 18.128.80.14
HPswitch(config)# vlan 10 ip access-group 50 in
HPswitch(config)# write mem
HPswitch(config)# show config
```

Startup configuration:

```
; J4850A Configuration Editor; Created on release #E.07.2%
hostname "HPswitch"
cdp run
module 1 type J4820A
ip routing
snmp-server community "public" Unrestricted
ip access-list standard "50"
   permit 18.128.100.10 0.0.0.0
   permit 18.128.100.27 0.0.0.0
   permit 18.128.80.14 0.0.0.0
   exit

vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A6,A19-A24
   ip address 15.30.248.180 255.255.248.0
   no untagged A7-A18
   exit

vlan 10
   name "VLAN_10"
   untagged A7-A12
   ip address 13.28.227.10 255.255.248.0
   ip access-group "50" in
   exit
```

9-36
Access Control Lists (ACLs)
Configuring and Assigning an ACL

- Denies IP traffic from the indicated IP address. Since, for this example, ACL 60 is a new list, this command also creates the ACL.
- Denies IP traffic from the indicated IP address.
- Permits IP traffic from all sources. (Traffic from the IP sources in the first two lines is already filtered and dropped.) The deny any with which the switch implicitly concludes all ACLs is preempted by this line.

Note: To enable traffic filtering with an ACL assigned to a VLAN such as the one shown in this example, IP routing must be enabled on the switch. Otherwise, no ACL filtering will occur.

Figure 9-12. Example of Configuring a Standard ACL To Deny Inbound Traffic from Specific IP Addresses
Configuring and Assigning a Numbered, Extended ACL

This section describes how to configure numbered, extended ACLs.

- To configure named ACLs, refer to “Configuring a Named ACL” on page 9-44.
- To configure standard, numbered ACL, refer to “Configuring and Assigning a Numbered, Standard ACL” on page 9-33.

While standard ACLs use only source IP addresses for filtering criteria, extended ACLs allow multiple ACE criteria. This enables you to more closely define your IP packet-filtering criteria. These criteria include:

- Source and destination IP addresses (required), in one of the following options:
  - Specific host IP
  - Subnet or group of IP addresses
  - Any IP address
- IP protocol (IP, TCP, or UDP)
- Source TCP or UDP port (if the IP protocol is TCP or UDP)
- Destination TCP or UDP port (if the IP protocol is TCP or UDP)
- TCP or UDP comparison operator (if the IP protocol is TCP or UDP)

You can configure up to 100 extended ACLs with a numeric name in the range of 100-199. You can also configure extended ACLs with alphanumeric names. (Refer to “Configuring a Named ACL” on page 9-44.) The switch allows a maximum of 255 ACLs in any combination of numeric and alphanumeric names, and determines the total from the number of unique ACL names in the configuration. For example, if you configure two ACLs, but assign only one of them to a VLAN, the ACL total is two, for the two unique ACL names. If you then assign the name of a nonexistent ACL to a VLAN, the new ACL total is three, because the switch now has three unique ACL names in its configuration. (The switch allows up to 1024 ACEs total in all ACLs.)

Note

**Syntax:** [no] access-list

Creates an ACE in the specified (100-199) access list and:

- Indicates the action (deny or permit) to take on a packet if there is a match between the packet and the criteria in the complete ACE.
- Specifies the packet protocol type (IP, TCP, or UDP).
- Specifies the source and destination addressing options described in the remainder of this section.
- Allows optional ACL logging where a packet has a match with a **deny** ACE.

If the ACL does not already exist, this command creates the specified ACL and its first ACE. If the ACL already exists, this command adds a new, explicit ACE to the end of the ACL. For a match to occur, the packet must have the source and destination IP addressing criteria specified by this command, as well as any protocol-specific (TCP or UDP port number) criteria specified by the command. To create a named ACL, refer to “Configuring a Named ACL” on page 9-44.

< 100-199>

**Specifies the ACL ID number:** The switch interprets an ACL with a value in this range as an extended ACL.

**Note:** To create an access list with an alphanumeric name instead of a number, refer to “Configuring a Named ACL” on page 9-44.

< deny | permit >

Specifies whether to deny (drop) or permit (forward) a packet that matches the ACE criteria.

< ip | tcp | udp >

**Specifies the packet protocol type required for a match:**

- **ip** — any IP packet
- **tcp** — only tcp packets
- **udp** — only udp packets
In an extended ACL, this parameter defines the source IP address (SA) that a packet must carry in order to have a match with the ACE.

- **any** — Specifies all inbound IP packets.
- **host < src-ip-addr >** — Specifies only inbound packets from a single IP address. Use this option when you want to match only the IP packets from one source IP address.
- **src-ip-addr/mask-length** — Performs the specified action on any IP packet having a source address within the range defined by either
  - < src-ip-addr / cidr-mask-bits >
  - or
  - < src-ip-addr < mask >>

Use this criterion to filter packets received from either a subnet or a group of IP addresses. The mask can be in either dotted-decimal format or CIDR format with the number of significant bits. Refer to “Using CIDR Notation To Enter the ACL Mask” on page 9-32.

The mask is applied to the IP address in the ACL to define which bits in a packet’s source IP address must exactly match the IP address configured in the ACL and which bits need not match. Note that specifying a group of contiguous IP addresses may require more than one ACE. For more on how masks operate in ACLs, refer to “How an ACE Uses a Mask To Screen Packets for Matches” on page 9-20.

[operator < src-port tcp/udp-id >]

In an extended ACL where you have selected either tcp or udp as the packet protocol type (see above), you can optionally use a TCP or UDP source port number or range of numbers to further define the criteria for a match. To specify a TCP or UDP port number, (1) select a comparison operator from the following list and (2) enter the port number or a well-known port name.
Comparison Operators:

- **eq <tcp/udp-port-nbr>** — “Equal To”; to have a match with the ACE entry, the TCP or UDP source port number in a packet must be equal to `<tcp/udp-port-nbr>`.
- **gt <tcp/udp-port-nbr>** — “Greater Than”; to have a match with the ACE entry, the TCP or UDP source port number in a packet must be greater than `<tcp/udp-port-nbr>`.
- **lt <tcp/udp-port-nbr>** — “Less Than”; to have a match with the ACE entry, the TCP or UDP source port number in a packet must be less than `<tcp/udp-port-nbr>`.
- **neq <tcp/udp-port-nbr>** — “Not Equal”; to have a match with the ACE entry, the TCP or UDP source port number in a packet must not be equal to `<tcp/udp-port-nbr>`.
- **range <start-port-nbr> < end-port-nbr>** — To have a match with the ACE entry, the TCP or UDP source port number in a packet must be in the range `<start-port-nbr> < end-port-nbr>`.

Port Number or Well-Known Port Name:

Use the TCP or UDP port number required by your application. The switch also accepts these well-known TCP or UDP port names as an alternative to their corresponding port numbers:

- **TCP**: bgp, dns, ftp, http, imap4, ldap, nntp, pop2, pop3, smtp, ssl, telnet
- **UDP**: bootpc, dns, ntp, radius, radius-old, rip, snmp, snmp-trap, tftp

*To list the above names, press the [Shift] [?] key combination after entering an operator. For a comprehensive listing of port numbers, visit www.iana.org/assignments/port-numbers.*

< any | host < dest-ip-addr | ip-addr/mask-length >

In an extended ACL, this parameter defines the destination IP address (DA) that a packet must carry in order to have a match with the ACE. The options are the same as shown for `<src-ip-addr>`.

[< dest-port tcp/udp-id >]

In an extended ACL, this parameter defines the TCP or UDP destination port number a packet must carry in order to have a match with the extended ACE. The options are the same as shown above on the preceding page for the source IP address.
Access Control Lists (ACLs)
Configuring and Assigning an ACL

[log]

Optional; generates an ACL log message if:

- The action is deny. (This option is not configurable for Permit.)
- There is a match.
- ACL logging is enabled on the switch. (Refer to “Enabling ACL Logging on the Switch” on page 9-60)

Syntax: `vlan < vid > ip access-group < list-# | ascii-str > < in | out >`

Assigns an ACL, designated by an ACL list number or ASCII string (alphanumeric list name), to a VLAN to filter either inbound or outbound IP traffic on that VLAN. To configure named ACLs, refer to “Configuring a Named ACL” on page 9-44.

Example of an Extended ACL. Suppose that you want to implement these policies on a Series 5300XL switch configured for IP routing and membership in VLANs 10, 20, and 30:

A. Permit Telnet traffic from 10.10.10.44 to 10.10.20.78, deny all other IP traffic from network 10.10.10.0 (VLAN 10) to 10.10.20.0 (VLAN 20), and permit all other IP traffic from any source to any destination. (See “A” in figure 9-13, below.)

B. Permit FTP traffic from IP address 10.10.20.100 (on VLAN 20) to 10.10.30.55 (on VLAN 30). Deny FTP traffic from other hosts on network 10.10.20.0 to any destination, but permit all other traffic.

Figure 9-13. Example of an Extended ACL
Access Control Lists (ACLs)
Configuring and Assigning an ACL

Figure 9-14. Example of Configuration Commands for an Extended ACL

```plaintext
HPswitch(config)# access-list 110 permit tcp host 10.10.10.44
    host 10.10.20.78 eq telnet
HPswitch(config)# access-list 110 deny ip 10.10.10.1 0.0.0.255 10.10.20.1 0.0.0.255
HPswitch(config)# access-list 110 permit ip any any
HPswitch(config)# vlan 10 ip access-group 110 in

HPswitch(config)# access-list 120 permit tcp host 10.10.20.100
    host 10.10.30.55 eq ftp
HPswitch(config)# access-list 120 deny tcp any any eq ftp
HPswitch(config)# access-list 120 permit ip any any
HPswitch(config)# vlan 20 ip access-group 120 in

HPswitch(config)# ip routing
HPswitch(config)# write mem
```

Enabling ip routing activates ACL operation on routed traffic.
Executing write memory saves the configuration changes to the startup-config file.
Configuring a Named ACL

You can use the “Named ACL” context to configure a standard or extended ACL with an alphanumeric name instead of a number. Note that the command structure for configuring a named ACL differs from that for a numbered ACL.

**Syntax:**

```
ip access-list standard < name-str | 1-99 >
   < deny | permit >
   < any | host < src-ip-addr > | ip-addr / mask-length >
   [ log ]

ip access-list extended < name-str | 100-199 >
   < deny | permit > ip
   < any | host < src-ip-addr > | ip-addr / mask-length >
   < any | host < dest-ip-addr > | ip-addr / mask-length >
   [ log ]

ip access-list extended < name-string >
   < deny | permit > < tcp | udp >
      < any | host < src-ip-addr > | ip-addr / mask-length >
      [ oper < src-port tcp/udp-id > ]
   < any | host < dest-ip-addr > | ip-addr / mask-length >
     [ oper < dest-port tcp/udp-id > ]
   [ log ]
```

*These commands create an ACE in the named ACL list and:*

- *Indicate the action (deny or permit) to take on a packet if there is a match between a packet and the criteria in the complete ACE.*
- *Specify the packet protocol type (IP, TCP, or UDP) and (if TCP or UDP) the comparison operator.*
- *Specify the source and destination addressing options required for a match.*
- *Allow optional ACL logging where a packet has a match with a deny ACE. The log option does not appear when permit is the action.*

*If the ACL does not already exist, these commands create the specified ACL and its first ACE. If the ACL already exists, these commands add a new, explicit ACE to the end of the ACL. For a match to occur, the packet must have the source and destination IP addressing criteria specified by this command, as well as any protocol-specific (TCP or UDP port number) criteria specified by the command.*
< name-str | 1-99 | 100-199 >

Consists of an alphanumeric string of up to 64 case-sensitive characters. If you include a space in the string, you must also enclose the string with quotes. For example, “ACL # 1”. You can also enter numbers in the ranges associated with standard (1-99) and extended (100-199) ACLs.

For explanations of the individual parameters in the preceding syntax statements, refer to the syntax descriptions under “Configuring and Assigning a Numbered, Standard ACL” on page 9-33 or “Configuring and Assigning a Numbered, Extended ACL” on page 9-38.

For example, figure 9-15 shows the commands for creating an ACL in the “Named ACL” context with these parameters:

<table>
<thead>
<tr>
<th>ACL Name:</th>
<th>VLAN 10 Inbound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action:</td>
<td>Deny</td>
</tr>
<tr>
<td>Protocol:</td>
<td>TCP</td>
</tr>
<tr>
<td>Source IP Address and Mask</td>
<td>10.10.20.100 0.0.0.0</td>
</tr>
<tr>
<td>Destination IP Address and Mask</td>
<td>10.10.10.1 0.0.0.255</td>
</tr>
<tr>
<td>Protocol Operator and Port Number at Destination</td>
<td>eq telnet</td>
</tr>
</tbody>
</table>
Enabling or Disabling ACL Filtering on a VLAN

For a given interface, you can configure one ACL to filter inbound traffic and one ACL to filter outbound traffic. You can also use the same ACL for both inbound and outbound traffic, and for assignment to multiple VLANs. For limits and operating rules, refer to “ACL Configuration and Operating Rules” on page 9-18.

Syntax:  

```
[no] vlan < vid > ip access-group < ascii-string > < in | out >
```

Assigns an ACL to a VLAN. You can use either the global configuration level or the VLAN context level to assign an ACL to a VLAN or remove an ACL from a VLAN.

**Note:** The switch allows you to assign a nonexistent ACL name or number to a VLAN. In this case, if you subsequently configure an ACL with that name or number, it will automatically become active on the assigned VLAN. Also, if you delete an assigned ACL from the switch without subsequently using the “no” form of this command to remove the assignment to a VLAN, the ACL assignment remains and will automatically activate any new ACE if you create with the same ACL name.
Access Control Lists (ACLs)

Deleting an ACL from the Switch

Syntax: 

no ip access-list standard < name-str | 1-99 >

no ip access-list extended < name-str | 100-199 >

Removes the specified ACL from the switch’s running-config file.

Note: Deleting an ACL does not delete any assignment of that ACL to a specific VLAN. If you need to delete an ACL assignment, refer to “Enabling or Disabling ACL Filtering on a VLAN” on page 9-46.
Displaying ACL Data

<table>
<thead>
<tr>
<th>ACL Commands</th>
<th>Function</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show access-list</td>
<td>View a brief listing of all ACLs on the switch.</td>
<td>9-48</td>
</tr>
<tr>
<td>show access-list config</td>
<td>Display the CLI commands for generating the ACL commands configured in the switch.</td>
<td>9-49</td>
</tr>
<tr>
<td>show access-list vlan &lt; vid &gt;</td>
<td>List the name and type of ACLs assigned to a particular VLAN on the switch.</td>
<td>9-50</td>
</tr>
<tr>
<td>show access-list &lt; acl-id &gt;</td>
<td>Display detailed content information for a specific ACL.</td>
<td>9-51</td>
</tr>
<tr>
<td>show config</td>
<td>show config includes configured ACLs and assignments existing in the startup-config file.</td>
<td></td>
</tr>
<tr>
<td>show running</td>
<td>show running includes configured ACLs and assignments existing in the running-config file.</td>
<td></td>
</tr>
</tbody>
</table>

Display an ACL Summary

This command lists the configured ACLs, regardless of whether they are assigned to any VLANs.

**Syntax:** show access-list

*List a summary table of the name, type, and application status of all ACLs configured on the switch.*

For example:

```
HPswitch(config)# show access-list

Access Control Lists

<table>
<thead>
<tr>
<th>Type</th>
<th>Appl</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>std</td>
<td>yes</td>
<td>1</td>
</tr>
<tr>
<td>ext</td>
<td>yes</td>
<td>103</td>
</tr>
<tr>
<td>ext</td>
<td>no</td>
<td>105</td>
</tr>
<tr>
<td>std</td>
<td>yes</td>
<td>Red VLAN Inbound</td>
</tr>
</tbody>
</table>

In this switch, ACLs 105 and “Red VLAN Inbound” exist in the configuration but are not applied to any VLANs and thus do not affect packet
```

**Figure 9-17. Example of a Summary Table of Access lists**

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Shows whether the listed ACL is std (Standard; source-address only) or ext (Extended; protocol, source, and destination data).</td>
</tr>
<tr>
<td>Appl</td>
<td>Shows whether the listed ACL has been applied to a VLAN (yes/no).</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the name or ID number assigned to each ACL configured in the switch.</td>
</tr>
</tbody>
</table>
Display the Content of All ACLs on the Switch

This command lists the configuration details for every ACL configured in the running-config file, regardless of whether you have assigned any to filter traffic on VLANs configured on the switch.

**Syntax:** `show access-list config`

List the configured syntax for all ACLs currently configured on the switch.

**Note**

Notice that you can use the output from this command for input to an offline text file in which you can edit, add, or delete ACL commands. Refer to “Editing ACLs and Creating an ACL Offline” on page 9-53.

This information also appears in the `show running` display. If you executed `write memory` after configuring an ACL, it appears in the `show config` display.

For example, with two ACLs configured in the switch, you will see results similar to the following:

```
HPswitch(config)# show access-list config
ip access-list standard "1"
  deny 18.28.236.77 0.0.0.0
  deny 18.29.140.107 0.0.0.0
  permit 0.0.0.0 255.255.255.255
exit
ip access-list extended "105"
  permit tcp 18.30.133.27 0.0.0.0 0.0.0.0 255.255.255.255
  permit tcp 18.30.155.101 0.0.0.0 0.0.0.0 255.255.255.255
  deny ip 18.30.133.1 0.0.0.255 0.0.0.0 255.255.255.255
  deny ip 18.30.155.1 0.0.0.255 0.0.0.0 255.255.255.255
  permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
```

Figure 9-18. Example of an ACL Configured Syntax Listing
Display the ACL Assignments for a VLAN

This command briefly lists the identification and type(s) of ACLs currently assigned to a particular VLAN in the running-config file. (The switch allows up to two ACL assignments per VLAN; one inbound and one outbound.)

**Syntax:** show access-list vlan < vid >

*List the ACLs assigned to a VLAN in the running config file.*

**Note**

This information also appears in the `show running` display. If you executed `write memory` after configuring an ACL, it appears in the `show config` display.

For example, if you assigned a standard ACL with an ACL-ID of “1” to filter inbound traffic on VLAN 10, you could quickly verify this assignment as follows:

```
HPswitch(config)# show access-list vlan 10

Access Lists for VLAN 10

  ( Inbound Access List: 1
    Type: Standard
  )

  Outbound Access List: none

```

*Figure 9-19. Example of Listing the ACL Assignments for a VLAN*
Displaying the Content of a Specific ACL

This command displays a specific ACL configured in the running config file in an easy-to-read tabular format.

**Note**

This information also appears in the `show running` display. If you executed `write memory` after configuring an ACL, it appears in the `show config` display.

**Syntax:** show access-list < acl-id >

Display detailed information on the content of a specific ACL configured in the running-config file.

For example, suppose you configured the following two ACLs in the switch:

<table>
<thead>
<tr>
<th>ACL ID</th>
<th>ACL Type</th>
<th>Desired Action</th>
</tr>
</thead>
</table>
| 1      | Standard | • Deny IP traffic from 18.28.236.77 and 18.29.140.107.  
• Permit IP traffic from all other sources. |
| 105    | Extended | • Permit any TCP traffic from 18.30.133.27 to any destination.  
• Deny any other IP traffic from 18.30.133.(1-255).  
• Permit all other IP traffic from any source to any destination. |

Inspect the ACLs as follows:
Access Control Lists (ACLs)

Displaying ACL Data

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The ACL identifier. Can be a number from 1 to 199, or a name.</td>
</tr>
<tr>
<td>Type</td>
<td>Standard or Extended. The former uses only source IP addressing. The latter uses both source and destination IP addressing and also allows TCP or UDP port specifiers.</td>
</tr>
<tr>
<td>Applied</td>
<td>“Yes” means the ACL has been applied to a VLAN. “No” means the ACL exists in the switch configuration, but has not been applied to any VLANs, and is therefore not in use.</td>
</tr>
<tr>
<td>ID</td>
<td>The sequential number of the Access Control Entry (ACE) in the specified ACL.</td>
</tr>
<tr>
<td>action</td>
<td>Permit (forward) or deny (drop) a packet when it is compared to the criteria in the applicable ACE and found to match.</td>
</tr>
</tbody>
</table>
| IP | **In Standard ACLs:** The source IP address to which the configured mask is applied to determine whether there is a match with a packet.  
**In Extended ACLs:** The source and destination IP addresses to which the corresponding configured masks are applied to determine whether there is a match with a packet. |
| Mask | The mask configured in an ACE and applied to the corresponding IP address in the ACE to determine whether a packet matches the filtering criteria. |
| proto | Used only in extended ACLs to specify the packet protocol type to filter. Must be either IP, TCP, or UDP. |
| oper | Used only in extended ACLs where a TCP or UDP port type and number have been entered. Specifies how to compare the corresponding TCP or UDP port number in a packet to the port number in the ACE. |
| port(s) | Used only in extended ACLs to show any TCP or UDP port number that has been entered in the ACE. |
| Log | Shows the status of logging for the entry (ACE). A blank space indicates ACL logging is not enabled for that ACE. |
Access Control Lists (ACLs)

Editing ACLs and Creating an ACL Offline

Display All ACLs and Their Assignments in the Switch Startup-Config File and Running-Config File

The `show config` and `show running` commands include in their listings any configured ACLs and any ACL assignments to VLANs. Refer to figure 9-11 (page 9-36) and figure 9-12 (page 9-37) for examples. Remember that `show config` lists the startup-config file and `show running` lists the running-config file.

Editing ACLs and Creating an ACL Offline

Earlier sections of this chapter describe how to use the CLI to create an ACL. Beginning with “Using the CLI To Edit ACLs”, below, describes how to use the CLI to edit existing ACLs. However, you can also create or edit an ACL offline, then use a TFTP server to upload the ACL as a command file. The offline method (page 9-56) provides a useful alternative to using the CLI for creating or editing large ACLs.

Using the CLI To Edit ACLs

The switch applies individual ACEs in the order in which they occur in an ACL. You can use the CLI to delete individual ACEs from anywhere in an ACL and to append new ACEs to the end of an ACL. However, the CLI method does not allow you to insert a new ACE between two existing ACEs.

Using the CLI To Edit a Short ACL. To insert a new ACE between existing ACEs in a short ACL, you may want to delete the ACL and then re-configure it by entering your updated list of ACEs in the correct order.

Using the CLI to Edit a Longer ACL. To insert a new ACE between existing ACEs in a longer ACL:

a. Delete the first ACE that is out of sequence and all following ACEs through the end of the ACL.

b. Re-Enter the desired ACEs in the correct sequence.
General Editing Rules

- You can delete any ACE from an ACL by repeating the ACE's entry command, preceded by the “no” statement. When you enter a new ACE, the switch inserts it as the last entry of the specified ACL.

- Deleting the last ACE from a numeric ACL, removes the ACL from the configuration. Deleting the last ACE from a named ACL leaves the ACL in memory. In this case, the ACL is “empty” and cannot perform any filtering tasks. (In any ACL the implicit “deny any” does not apply unless the ACL includes at least one explicit ACE.)

- When you create a new ACL, the switch inserts it as the last ACL in the startup-config file. (Executing **write memory** saves the running-config file to the startup-config file.)

Deleting Any ACE from an ACL

You can delete an ACE from an ACL by repeating the ACE's entry command, preceded by the “no” statement.

**Syntax:**

```plaintext
no access-list < acl-id > < permit | deny > < any | host | ip-addr/mask-length >
```

*Deletes an ACE from a standard ACL. All variable parameters in the command must be an exact match with their counterparts in the ACE you want to delete.*

```plaintext
no access-list < acl-id > < permit | deny > < ip | tcp | udp > < src-addr: any | host | ip-addr/mask-length > [operator < src-port-num >]
< dest-addr: any | host | ip-addr-mask-length > [operator < dest-port-num > [log]]
```

*Deletes an ACE from a standard ACL. All variable parameters in the command must be an exact match with their counterparts in the ACE you want to delete.*
For example, the first of the following two commands creates an ACE in ACL 22 and the second deletes the same ACE:

```
HPswitch(config)# access-list 22 permit host 18.28.152.64
HPswitch(config)# no access-list 22 permit host 18.28.152.64
```

Figure 9-21. Example of Deleting an ACE from a Standard ACL

Figure 9-22 shows an example of deleting an ACE from an extended ACL.

```
HPswitch(config)# show config
!Startup configuration:
 !
!ip access-list extended "103"
   deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
   deny tcp 0.0.0.0 255.255.255.255 10.10.20.2 0.0.0.0 eq 23 log
   permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit
!vlan 1
   name "DEFAULT_VLAN"
   untagged A1

ACL 103 Before Removing the Second "deny" ACE.

ACL 103 After Removing the Second "deny" ACE.

HPswitch(config)# no access-list 103 deny tcp any host 10.10.20.2 eq 23 log
HPswitch(config)# write mem
HPswitch(config)# show config
!Startup configuration:
 !
!ip access-list extended "103"
   deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
   permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
   exit
!vlan 1
   name "DEFAULT_VLAN"
   untagged A1

ACL 103 Before Removing the Second "deny" ACE.

Use no access-list to remove this line from ACL 103.

ACL 103 After Removing the Second "deny" ACE.

Figure 9-22. Example of Deleting an ACE from an ACL
**Working Offline To Create or Edit an ACL**

For longer ACLs that would be difficult or time-consuming to accurately create or edit in the CLI, you can use the offline method:

1. Begin by doing one of the following:
   - To edit one or more existing ACLs, use `copy command-output tftp` to copy the current version of the ACL configuration to a file in your TFTP server. For example, to copy the ACL configuration to a file named `acl02.txt` in the TFTP directory on a server at 18.28.227.2:
     ```
     HPswitch# copy command-output 'show access-list config' tftp 18.28.227.2 acl02.txt pc
     ```
   - To create a new ACL, just open a text file in the appropriate directory on a TFTP server accessible to the switch.

2. Use the text editor to create or edit the ACL(s).

3. Use `copy tftp command-file` to download the file as a list of commands to the switch.

**Creating an ACL Offline**

Use a text editor that allows you to create an ASCII text file (.txt).

If you are replacing an ACL on the switch with a new ACL that uses the same number or name syntax, begin the command file with a “no” command to remove the earlier version of the ACL from the switch’s running-config file. Otherwise, the switch will append the new ACEs in the ACL you download to the existing ACL. For example, if you plan to use the Copy command to replace ACL “103”, you would place this command at the beginning of the edited file:

```plaintext
no ip access-list extended 103
```

- Removes an existing ACL and replaces it with a new version with the same identity.
- To append new ACEs to the ACL instead of replacing it, you would omit the first line.

**Figure 9-23. Example of an Offline ACL File Designed To Replace An Existing ACL**

```plaintext
no ip access-list extended 103
ip access-list extended "103"
  deny tcp 0.0.0.0 255.255.255.255 10.10.10.2 0.0.0.0 eq 23 log
  permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
exit
```
For example, suppose that you wanted to create an extended ACL to fulfill the following requirements (Assume a subnet mask of 255.255.255.0):

- ID: “Controls for VLAN 20"
- Deny Telnet access to a server at 10.10.10.100 on VLAN 10 from these three IP addresses on VLAN 20 (with ACL logging):
  - 10.10.20.17
  - 10.10.20.23
  - 10.10.20.40
- Allow any access to the server from all other addresses on VLAN 20:
- Permit internet access to these two IP address on VLAN 20, but deny access to all other addresses on VLAN 20 (without ACL logging).
  - 10.10.20.98
  - 10.10.20.21
- Deny all other traffic from VLAN 20 to VLAN 10.
- Deny all traffic from VLAN 30 (10.10.30.0) to the server at 10.10.10.100 on VLAN 10 (without ACL logging), but allow any other traffic from VLAN 30 to VLAN 10.
- Deny all other inbound traffic to VLAN 20. (Hint: The implicit “deny any” can achieve this objective.)

1. You would create a .txt file with the content shown in figure 9-24.
Access Control Lists (ACLs)
Editing ACLs and Creating an ACL Offline

Enables a comment in the file.

You can use the ";" character to denote a comment. The file stored on your TFTP server retains comments, and they appear when you use copy to download the ACL command file. (Comments are not saved in the switch configuration.)

Blank lines in the file cause breaks in the displayed line-numbering sequence when you copy the command file to the switch. This is normal operation. (See figure 9-25.)

Figure 9-24. Example of a.txt File Designed for Creating an ACL

2. After you copy the above .txt file to a TFTP server the switch can access, you would then execute the following command:

```
HPswitch(config)# copy tftp command-file 13.28.227.2 acl-vlan20.txt pc
Running configuration may change, do you want to continue [y/n]? y
1. ip access-list extended "153"
3. ; APPLIES INBOUND ON VLAN 20.
6. ; ANY SOURCE TO VLAN 20 DESTINATIONS.
    permit tcp 0.0.0.0 255.255.255.255 10.10.20.98 0.0.0.0 eq http
    permit tcp 0.0.0.0 255.255.255.255 10.10.20.21 0.0.0.0 eq http
    deny tcp 0.0.0.0 255.255.255.255 10.10.20.1 0.0.0.255 eq http
  7. ; VLAN 20 SOURCES TO VLAN 10 DESTINATIONS.
    deny tcp 10.10.20.17 0.0.0.0 10.10.10.100 0.0.0.0 eq telnet log
    deny tcp 10.10.20.23 0.0.0.0 10.10.10.100 0.0.0.0 eq telnet log
    deny tcp 10.10.20.40 0.0.0.0 10.10.10.100 0.0.0.0 eq telnet log
    permit ip 10.10.20.1 0.0.0.255 10.10.10.100 0.0.0.0
  8. ; VLAN 30 POLICY.
    deny ip 10.10.30.1 0.0.0.255 10.10.10.100 0.0.0.0
    permit ip 10.10.30.1 0.0.0.255 10.10.10.100 0.0.0.0
exit
vlan 20 ip access-group "Controls for VLAN 20" in
```

Figure 9-25. Example of Using "copy tftp command-file" To Configure an ACL in the Switch
If a transport error occurs, the switch does not execute the command and the ACL is not configured.

3. Next, assign the new ACL to the intended VLAN which, in this example, is for inbound traffic on VLAN 20.

   HPswitch(config)# vlan 20 ip access-group "Controls for VLAN 20" in

4. Inspect the new running configuration:

   HPswitch(config)# show running

5. If the configuration appears satisfactory, save it to the startup-config file:

   HPswitch(config)# write memory

---

**Enable ACL “Deny” Logging**

ACL logging enables the switch to generate a message when IP traffic meets the criteria for a match with an ACE that results in an explicit “deny” action. You can use ACL logging to help:

- Test your network to ensure that your ACL configuration is detecting and denying the traffic you do not want forwarded
- Receive notification when the switch detects attempts to transmit traffic you have designed your ACLs to reject

The switch sends ACL messages to Syslog and optionally to the current console, Telnet, or SSH session. You can configure up to six Syslog server destinations.

**Requirements for Using ACL Logging**

- The switch configuration must include an ACL (1) assigned to a static VLAN and (2) containing an ACE configured with the `deny` action and the `log` option.
- To screen routed packets with destination IP addresses outside of the switch, IP routing must be enabled.
- For ACL logging to a Syslog server, the server must be accessible to the switch and identified (with the `logging <ip-addr>` command) in the switch configuration.
Debug must be enabled for ACLs and one or both of the following:
- logging (for sending messages to Syslog)
- Session (for sending messages to the current console interface)

ACL Logging Operation

When the switch detects a packet match with an ACE and the ACE includes both the **deny** action and the optional **log** parameter, an ACL log message is sent to the designated debug destination. The first time a packet matches an ACE with **deny** and **log** configured, the message is sent immediately to the destination and the switch starts a wait-period of approximately five minutes. (The exact duration of the period depends on how the packets are internally routed.) At the end of the collection period, the switch sends a single-line summary of any additional “deny” matches for that ACE (and any other “deny” ACEs for which the switch detected a match). If no further log messages are generated in the wait-period, the switch suspends the timer and resets itself to send a message as soon as a new “deny” match occurs. The data in the message includes the information illustrated in figure 9-26.

```
Mar 1 10:04:45 18.28.227.101 ACL:
_ACL 03/01/03 10:04:45: denied tcp 13.28.227.3 (1025) (VLAN 227) -> 10.10.20.2 (23), 1 packets
```

**Figure 9-26. Content of an ACL-Generated Message**

Enabling ACL Logging on the Switch

1. Use the debug command to:
   a. Configure one or more log destinations.
Enable ACL “Deny” Logging

b. If you are using a Syslog server, use the **logging** command to configure the server's IP address. (You can configure up to six Syslog servers.)

c. Ensure that the switch can access any Syslog servers you specify.

2. Configure one or more ACLs with the deny action and the log option.

For example, suppose that you want to:

- On VLAN 100 configure an extended ACL with an ACL-ID of 143 to deny Telnet traffic from IP address 18.38.100.127 on VLAN 100.

- Configure the switch to send an ACL log message to the console and to a Syslog server at IP address 18.38.110.54 on VLAN 110 if the switch detects a match denying Telnet access from 18.38.100.127.

(This example assumes that IP routing is already configured on the switch.)

![Diagram](image_url)

**Figure 9-27. Example of an ACL Log Application**
Access Control Lists (ACLs)
Enable ACL “Deny” Logging

Access Control Lists (ACLs)
Enable ACL “Deny” Logging

Operating Notes for ACL Logging

- The ACL logging feature generates a message only when packets are explicitly denied as the result of a match, and not when explicitly permitted or implicitly denied. To help test ACL logging, configure an ACL with an explicit deny any and log statements at the end of the list, and apply the ACL to an appropriate VLAN.

- Logging enables you to selectively test specific devices or groups. However, excessive logging can affect switch performance. For this reason, HP recommends that you remove the logging option from ACEs for which you do not have a present need. Also, avoid configuring logging where it does not serve an immediate purpose. (Note that ACL logging is not designed to function as an accounting method.) See also "Apparent Failure To Log All "Deny" Matches" in the section titled “ACL Problems”, found in appendix C, “Troubleshooting” of the Management and Configuration Guide for your switch.

- When configuring logging, you can reduce excessive use by configuring the appropriate ACEs to match with specific hosts instead of entire subnets.

Figure 9-28. Commands for Applying an ACL with Logging to Figure 9-27

```bash
HPswitch(config)# access-list 143 deny tcp host 18.38.100.127 any eq telnet log
HPswitch(config)# access-list 143 permit ip any any
HPswitch(config)# vlan 100 ip access-group 143 in
HPswitch(config)# logging 18.38.110.54
HPswitch(config)# debug acl
HPswitch(config)# debug destination logging
HPswitch(config)# debug destination session
HPswitch(config)# write memory
HPswitch(config)# show debug
```

Debug Logging
Destination:
   Logging
   18.38.110.54
   Session
   Enabled debug types:
   event
   acl log
General ACL Operating Notes

ACLs do not provide DNS hostname support.

Protocol Support: ACL criteria includes IP, TCP, and UDP. ACLs do not use these protocols:

- TOS (Type-of-Service)
- Precedence
- MAC information
- QoS

ACLs do not affect switch serial port access.

When the ACL configuration includes TCP or UDP options, the switch operates in “strict” TCP and UDP mode for increased control. The switch compares all TCP and UDP packets against the ACLs. (In the HP Series 9300 Routing Switches, the Strict TCP and Strict UDP modes are optional and must be specifically invoked.)

Replacing or Adding To an Active ACL Policy. If you assign an ACL to a VLAN and subsequently add or replace ACEs in that ACL, each new ACE becomes active when you enter it.

Note

When an ACE becomes active, it screens the packets resulting from new traffic connections. It does not screen packets resulting from currently open traffic connections. If you invoke a new ACE to screen packets in a currently open traffic connection, you must force the connection to close before the ACE can begin screening packets from that source.

ACL Screening of Traffic Generated by the Switch. Outbound ACLs on a switch do not screen traffic (such as broadcasts, Telnet, Ping, and ICMP replies) generated by the switch itself. Note that ACLs do screen this type of traffic when other devices generate it. Similarly, ACLs can screen responses from other devices to unscreened traffic the switch generates.
This page is intentionally unused.
IP Routing Features

Contents

Overview of IP Routing .................................................. 10-3
  IP Interfaces ......................................................... 10-4
  IP Tables and Caches ............................................... 10-4
  IP Route Exchange Protocols ..................................... 10-7
  IP Global Parameters for Routing Switches .................... 10-7
  IP Interface Parameters for Routing Switches .............. 10-9

Configuring IP Parameters for Routing Switches ............. 10-10
  Configuring IP Addresses ........................................ 10-10
  Changing the Router ID ........................................... 10-10
  Configuring ARP Parameters .................................... 10-11
  Configuring Forwarding Parameters ......................... 10-13
  Configuring ICMP .................................................. 10-15

Configuring Static IP Routes ....................................... 10-17
  Static Route Types ............................................... 10-17
  Static IP Route Parameters ..................................... 10-18
  Static Route States Follow Port States ..................... 10-18
  Configuring a Static IP Route ................................ 10-19
  Configuring a “Null” Route ..................................... 10-19

Configuring RIP ........................................................ 10-21
  Overview of RIP ................................................... 10-21
  RIP Parameters and Defaults .................................... 10-22
  Configuring RIP Parameters ..................................... 10-23
  Configuring RIP Redistribution ................................ 10-25
  Changing the Route Loop Prevention Method ............... 10-27
  Displaying RIP Information ................................. 10-27
Configuring OSPF ....................................................... 10-34
  Overview of OSPF .................................................. 10-34
  Configuring OSPF .................................................. 10-38
  Displaying OSPF Information ..................................... 10-53

Configuring IRDP ..................................................... 10-70
  Enabling IRDP Globally ............................................ 10-71
  Enabling IRDP on an Individual VLAN Interface ............... 10-71
  Displaying IRDP Information ..................................... 10-72

Configuring DHCP Relay .............................................. 10-73
  Overview ............................................................. 10-73
  DHCP Packet Forwarding .......................................... 10-73
  Minimum Requirements for DHCP Relay Operation ............ 10-74

Configuring Static Network Address Translation (NAT) for Intranet Applications ........................................... 10-76
  Static NAT Operating Rules ....................................... 10-77
  Configuring Static NAT ............................................ 10-77
  Displaying Static NAT Statistics and Configuration .......... 10-79
  Static NAT Operating Notes ....................................... 10-79
Overview of IP Routing

The HP Procurve Series 5300XL Switches offer the following IP routing features:

- **IP Static Routes** – supports up to 256 static routes
- **RIP** (Router Information Protocol) – supports RIP Version 1, Version 1 compatible with Version 2 (default), and Version 2
- **OSPF** (Open Shortest Path First) – the standard routing protocol for handling larger routed networks
- **IRDP** (ICMP Router Discovery Protocol) – advertises the IP addresses of the routing interfaces on this switch to directly attached host systems
- **DHCP Relay** – allows you to extend the service range of your DHCP server beyond its single local network segment

All these features are configurable through the switch’s console CLI.

Throughout this chapter, the HP Procurve Series 5300XL Switches will be referred to as “routing switches”. When IP routing is enabled on your switch, it behaves just like any other IP router.

Basic IP routing configuration consists of adding IP addresses, enabling IP routing, and, enabling a route exchange protocol, such as Routing Information Protocol (RIP).

For configuring the IP addresses, see chapter 7, “Configuring IP Addresses”. The rest of this chapter describes IP routing and how to configure it in more detail. Use the information in this chapter if you need to change some of the IP parameters from their default values or you want to view configuration information or statistics.
IP Interfaces

On the routing switches, IP addresses are associated with individual VLANs. By default, there is a single VLAN (Default_VLAN) on the routing switch. In that configuration, a single IP address serves as the management access address for the entire device. If routing is enabled on the routing switch, the IP address on the single VLAN also acts as the routing interface.

Each IP address on a routing switch must be in a different sub-net. You can have only one VLAN interface that is in a given sub-net. For example, you can configure IP addresses 192.168.1.1/24 and 192.168.2.1/24 on the same routing switch, but you cannot configure 192.168.1.1/24 and 192.168.1.2/24 on the same routing switch.

You can configure multiple IP addresses on the same VLAN.

The number of IP addresses you can configure on an individual VLAN interface is 8.

You can use any of the IP addresses you configure on the routing switch for Telnet, Web management, or SNMP access, as well as for routing.

Note

All HP Procurve devices support configuration and display of IP address in classical sub-net format (example: 192.168.1.1 255.255.255.0) and Classless Interdomain Routing (CIDR) format (example: 192.168.1.1/24). You can use either format when configuring IP address information. IP addresses are displayed in classical sub-net format only.

IP Tables and Caches

The following sections describe the IP tables and caches:

- ARP cache table
- IP route table
- IP forwarding cache

The software enables you to display these tables.
ARP Cache Table

The ARP cache contains entries that map IP addresses to MAC addresses. Generally, the entries are for devices that are directly attached to the routing switch.

An exception is an ARP entry for an interface-based static IP route that goes to a destination that is one or more router hops away. For this type of entry, the MAC address is either the destination device’s MAC address or the MAC address of the router interface that answered an ARP request on behalf of the device, using proxy ARP.

**ARP Cache.** The ARP cache contains dynamic (learned) entries. The software places a dynamic entry in the ARP cache when the routing switch learns a device’s MAC address from an ARP request or ARP reply from the device.

The software can learn an entry when the switch or routing switch receives an ARP request from another IP forwarding device or an ARP reply. Here is an example of a dynamic entry:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>207.95.6.102</td>
<td>0800.5afc.ea21</td>
<td>Dynamic</td>
<td>6</td>
</tr>
</tbody>
</table>

Each entry contains the destination device’s IP address and MAC address.

To configure other ARP parameters, see “Configuring ARP Parameters” on page 10-11.

IP Route Table

The IP route table contains routing paths to IP destinations.

**Note**

The default gateway, which you specify when you configure the basic IP information on the switch, is used only when routing is not enabled on the switch.

The IP route table can receive the routing paths from the following sources:

- A directly-connected destination, which means there are no router hops to the destination
- A static IP route, which is a user-configured route
- A route learned through RIP
- A route learned through OSPF
The IP route table contains the best path to a destination.

- When the software receives paths from more than one of the sources listed above, the software compares the administrative distance of each path and selects the path with the lowest administrative distance. The administrative distance is a protocol-independent value from 1 – 255.

The IP route table is displayed by entering the CLI command **show ip route** from any context level in the console CLI. Here is an example of an entry in the IP route table:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Network Mask</th>
<th>Gateway</th>
<th>Type</th>
<th>Sub-Type</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>connected</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Each IP route table entry contains the destination’s IP address and sub-net mask and the IP address of the next-hop router interface to the destination. Each entry also indicates route type, and for OSPF routes, the sub type, and the route’s IP metric (cost). The type indicates how the IP route table received the route.

To configure a static IP route, see “Configuring a Static IP Route” on page 10-19

**IP Forwarding Cache**

The IP forwarding cache provides a fast-path mechanism for forwarding IP packets. The cache contains entries for IP destinations. When an HP ProCurve routing switch has completed processing and addressing for a packet and is ready to forward the packet, the device checks the IP forwarding cache for an entry to the packet’s destination.

- If the cache contains an entry with the destination IP address, the device uses the information in the entry to forward the packet out the ports listed in the entry. The destination IP address is the address of the packet’s final destination. The port numbers are the ports through which the destination can be reached.

- If the cache does not contain an entry, the software can create an entry in the forwarding cache.

Each entry in the IP forwarding cache has an age timer. If the entry remains unused for five minutes, the software removes the entry. The age timer is not configurable.

**Note**

You cannot add static entries to the IP forwarding cache.
IP Route Exchange Protocols

HP Procurve Series 5300XL Switches support the following IP route exchange protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)

These protocols provide routes to the IP route table. You can use one or more of these protocols, in any combination. The protocols are disabled by default. For configuration information, see the following:

- “Configuring RIP” on page 10-21
- “Configuring OSPF” on page 10-34

IP Global Parameters for Routing Switches

The following table lists the IP global parameters and the page where you can find more information about each parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The value that routers use to identify themselves to other routers when exchanging route information. OSPF uses the router ID to identify routers. RIP does not use the router ID.</td>
<td>The lowest-numbered IP address configured on the lowest-numbered routing interface.</td>
<td>10-10</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP)</td>
<td>A standard IP mechanism that routers use to learn the Media Access Control (MAC) address of a device on the network. The router sends the IP address of a device in the ARP request and receives the device’s MAC address in an ARP reply.</td>
<td>Enabled</td>
<td>10-11</td>
</tr>
<tr>
<td>ARP age</td>
<td>The amount of time the device keeps a MAC address learned through ARP in the device’s ARP cache. The device resets the timer to zero each time the ARP entry is refreshed and removes the entry if the timer reaches the ARP age.</td>
<td>Five minutes</td>
<td>not configurable</td>
</tr>
<tr>
<td>Proxy ARP</td>
<td>An IP mechanism a router can use to answer an ARP request on behalf of a host, by replying with the router’s own MAC address instead of the host’s.</td>
<td>Disabled</td>
<td>10-13</td>
</tr>
</tbody>
</table>
### Parameter | Description | Default | See page
--- | --- | --- | ---
Time to Live (TTL) | The maximum number of routers (hops) through which a packet can pass before being discarded. Each router decreases a packet’s TTL by 1 before forwarding the packet. If decreasing the TTL causes the TTL to be 0, the router drops the packet instead of forwarding it. | 64 hops | Refer to the chapter titled “Configuring IP Addressing” in the Management and Configuration Guide. |
Directed broadcast forwarding | A directed broadcast is a packet containing all ones (or in some cases, all zeros) in the host portion of the destination IP address. When a router forwards such a broadcast, it sends a copy of the packet out each of its enabled IP interfaces. **Note:** You also can enable or disable this parameter on an individual interface basis. See table 10-2 on page 10-9. | Disabled | 10-14 |
ICMP Router Discovery Protocol (IRDP) | An IP protocol that a router can use to advertise the IP addresses of its router interfaces to directly attached hosts. You can enable or disable the protocol at the Global CLI Config level. You also can enable or disable IRDP and configure the following protocol parameters on an individual VLAN interface basis at the VLAN Interface CLI Config level.  
- Forwarding method (broadcast or multicast)  
- Hold time  
- Maximum advertisement interval  
- Minimum advertisement interval  
- Router preference level | Disabled | 10-70 10-71 |
Static route | An IP route you place in the IP route table. | No entries | 10-17 |
Default network route | The router uses the default network route if the IP route table does not contain a route to the destination. For the Series 5300XL Switches, enter an explicit default route (0.0.0.0 0.0.0.0 or 0.0.0.0/0) as a static route in the IP route table. | None configured | 10-19 |
### IP Interface Parameters for Routing Switches

Table 10-2 lists the interface-level IP parameters for routing switches.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>A Layer 3 network interface address; separate IP addresses on individual VLAN interfaces.</td>
<td>None configured</td>
<td>chapter 7</td>
</tr>
<tr>
<td>Metric</td>
<td>A numeric cost the router adds to RIP routes learned on the interface. This parameter applies only to RIP routes.</td>
<td>1 (one)</td>
<td>10-23</td>
</tr>
<tr>
<td>ICMP Router Discovery Protocol (IRDP)</td>
<td>Locally overrides the global IRDP settings. See table 10-1 on page 10-7 for global IRDP information.</td>
<td>Disabled</td>
<td>10-71</td>
</tr>
<tr>
<td>IP helper address</td>
<td>The IP address of a UDP application server (such as a BootP or DHCP server) or a directed broadcast address. IP helper addresses allow the routing switch to forward requests for certain UDP applications from a client on one sub-net to a server on another sub-net.</td>
<td>None configured</td>
<td>10-74</td>
</tr>
</tbody>
</table>
Configuring IP Parameters for Routing Switches

The following sections describe how to configure IP parameters. Some parameters can be configured globally while others can be configured on individual VLAN interfaces. Some parameters can be configured globally and overridden for individual VLAN interfaces.

**Note**

This section describes how to configure IP parameters for routing switches. For IP configuration information when routing is not enabled, see chapter 7, “Configuring IP Addressing”.

### Configuring IP Addresses

You can configure an IP address on the routing switch’s VLAN interfaces. Configuring IP addresses is described in detail in chapter 7, “Configuring IP Addressing”.

### Changing the Router ID

In most configurations, a routing switch has multiple IP addresses, usually configured on different VLAN interfaces. As a result, a routing switch’s identity to other devices varies depending on the interface to which the other device is attached. Some routing protocols, including Open Shortest Path First (OSPF), identify a routing switch by just one of the IP addresses configured on the routing switch, regardless of the interfaces that connect the routing switches. This IP address is the router ID.

**Note**

Routing Information Protocol (RIP) does not use the router ID.

By default, the router ID on an HP routing switch is the lowest numbered IP interface configured on the device.

If you prefer, you can explicitly set the router ID to any valid IP address. The IP address cannot be in use on another device in the network.

**Note**

To display the router ID, enter the `show ip ospf` CLI command at any Manager EXEC CLI level.
To change the router ID, enter a command such as the following:

HPswitch(config)# ip router-id 209.157.22.26

**Syntax:** Syntax: ip router-id <ip-addr>

The <ip-addr> can be any valid, unique IP address.

---

**Note**

You can specify an IP address used for an interface on the HP routing switch, but do not specify an IP address in use by another device.

---

### Configuring ARP Parameters

Address Resolution Protocol (ARP) is a standard IP protocol that enables an IP routing switch to obtain the MAC address of another device’s interface when the routing switch knows the IP address of the interface. ARP is enabled by default and cannot be disabled.

**How ARP Works**

A routing switch needs to know a destination’s MAC address when forwarding traffic, because the routing switch encapsulates the IP packet in a Layer 2 packet (MAC layer packet) and sends the Layer 2 packet to a MAC interface on a device directly attached to the routing switch. The device can be the packet’s final destination or the next-hop router toward the destination.

The routing switch encapsulates IP packets in Layer 2 packets regardless of whether the ultimate destination is locally attached or is multiple router hops away. Since the routing switch’s IP route table and IP forwarding cache contain IP address information but not MAC address information, the routing switch cannot forward IP packets based solely on the information in the route table or forwarding cache. The routing switch needs to know the MAC address that corresponds with the IP address of either the packet’s locally attached destination or the next-hop router that leads to the destination.

For example, to forward a packet whose destination is multiple router hops away, the routing switch must send the packet to the next-hop router toward its destination, or to a default route or default network route if the IP route table does not contain a route to the packet’s destination. In each case, the routing switch must encapsulate the packet and address it to the MAC address of a locally attached device, the next-hop router toward the IP packet’s destination.
To obtain the MAC address required for forwarding a datagram, the routing switch does the following:

- First, the routing switch looks in the ARP cache (not the static ARP table) for an entry that lists the MAC address for the IP address. The ARP cache maps IP addresses to MAC addresses. The cache also lists the port attached to the device and, if the entry is dynamic, the age of the entry. A dynamic ARP entry enters the cache when the routing switch receives an ARP reply or receives an ARP request (which contains the sender’s IP address and MAC address). A static entry enters the ARP cache from the static ARP table (which is a separate table) when the interface for the entry comes up.

To ensure the accuracy of the ARP cache, each dynamic entry has its own age timer. The timer is reset to zero each time the routing switch receives an ARP reply or ARP request containing the IP address and MAC address of the entry. If a dynamic entry reaches its maximum allowable age, the entry times out and the software removes the entry from the table. Static entries do not age out and can be removed only by you.

- If the ARP cache does not contain an entry for the destination IP address, the routing switch broadcasts an ARP request out all its IP interfaces. The ARP request contains the IP address of the destination. If the device with the IP address is directly attached to the routing switch, the device sends an ARP response containing its MAC address. The response is a unicast packet addressed directly to the routing switch. The routing switch places the information from the ARP response into the ARP cache.

ARP requests contain the IP address and MAC address of the sender, so all devices that receive the request learn the MAC address and IP address of the sender and can update their own ARP caches accordingly.

**Note:** The ARP request broadcast is a MAC broadcast, which means the broadcast goes only to devices that are directly attached to the routing switch. A MAC broadcast is not routed to other networks. However, some routers, including HP routing switches, can be configured to reply to ARP requests from one network on behalf of devices on another network. See “Enabling Proxy ARP” below.

**Note**

If the routing switch receives an ARP request packet that it is unable to deliver to the final destination because of the ARP time-out and no ARP response is received (the routing switch knows of no route to the destination address), the routing switch sends an ICMP Host Unreachable message to the source.
Enabling Proxy ARP

Proxy ARP allows a routing switch to answer ARP requests from devices on one network on behalf of devices in another network. Since ARP requests are MAC-layer broadcasts, they reach only the devices that are directly connected to the sender of the ARP request. Thus, ARP requests do not cross routers.

For example, if Proxy ARP is enabled on a routing switch connected to two sub-nets, 10.10.10.0/24 and 20.20.20.0/24, the routing switch can respond to an ARP request from 10.10.10.69 for the MAC address of the device with IP address 20.20.20.69. In standard ARP, a request from a device in the 10.10.10.0/24 sub-net cannot reach a device in the 20.20.20.0 sub-net if the sub-nets are on different network cables, and thus is not answered.

An ARP request from one sub-net can reach another sub-net when both sub-nets are on the same physical segment (Ethernet cable), since MAC-layer broadcasts reach all the devices on the segment.

Proxy ARP is disabled by default on HP routing switches. To enable Proxy ARP, enter the following commands from the VLAN context level in the CLI:

```
HPswitch(config)# vlan 1
HPswitch(vlan-1)# ip proxy-arp
```

To again disable IP proxy ARP, enter the following command:

```
HPswitch(vlan-1)# no ip proxy-arp
```

**Syntax:** `[no] ip proxy-arp`

Configuring Forwarding Parameters

The following configurable parameters control the forwarding behavior of HP routing switches:

- Time-To-Live (TTL) threshold
- Forwarding of directed broadcasts

All these parameters are global and thus affect all IP interfaces configured on the routing switch.

To configure these parameters, use the procedures in the following sections.
Changing the TTL Threshold

The configuration of this parameter is covered in chapter 7, “Configuring IP Addressing”.

Enabling Forwarding of Directed Broadcasts

A directed broadcast is an IP broadcast to all devices within a single directly-attached network or sub-net. A net-directed broadcast goes to all devices on a given network. A sub-net-directed broadcast goes to all devices within a given sub-net.

Note

A less common type, the all-sub-nets broadcast, goes to all directly-attached sub-nets. Forwarding for this broadcast type also is supported, but most networks use IP multicasting instead of all-sub-net broadcasting.

Forwarding for all types of IP directed broadcasts is disabled by default. You can enable forwarding for all types if needed. You cannot enable forwarding for specific broadcast types.

To enable forwarding of IP directed broadcasts, enter the following CLI command:

```
HPswitch(config)# ip directed-broadcast
```

**Syntax:** [no] ip directed-broadcast

HP software makes the forwarding decision based on the routing switch's knowledge of the destination network prefix. Routers cannot determine that a message is unicast or directed broadcast apart from the destination network prefix. The decision to forward or not forward the message is by definition only possible in the last hop router.

To disable the directed broadcasts, enter the following CLI command:

```
HPswitch(config)# no ip directed-broadcast
```
Configuring ICMP

You can configure the following ICMP limits:

- **Burst-Normal** – The maximum number of ICMP replies to send per second.
- **Reply Limit** – You can enable or disable ICMP reply rate limiting.

Disabling ICMP Messages

HP devices are enabled to reply to ICMP echo messages and send ICMP Destination Unreachable messages by default.

You can selectively disable the following types of Internet Control Message Protocol (ICMP) messages:

- **Echo messages** (ping messages) – The routing switch replies to IP pings from other IP devices.
- **Destination Unreachable messages** – If the routing switch receives an IP packet that it cannot deliver to its destination, the routing switch discards the packet and sends a message back to the device that sent the packet to the routing switch. The message informs the device that the destination cannot be reached by the routing switch.
- **Address Mask replies** – You can enable or disable ICMP address mask replies.

Disabling Replies to Broadcast Ping Requests

By default, HP devices are enabled to respond to broadcast ICMP echo packets, which are ping requests. You can disable response to ping requests on a global basis using the following CLI method.

To disable response to broadcast ICMP echo packets (ping requests), enter the following command:

```
HPswitch(config)# no ip icmp echo broadcast-request
```

**Syntax:** `[no] ip icmp echo broadcast-request`

If you need to re-enable response to ping requests, enter the following command:

```
HPswitch(config)# ip icmp echo broadcast-request
```
Disabling ICMP Destination Unreachable Messages

By default, when an HP device receives an IP packet that the device cannot deliver, the device sends an ICMP Unreachable message back to the host that sent the packet. The following types of ICMP Unreachable messages are generated:

- Administration – The packet was dropped by the HP device due to a filter or ACL configured on the device.
- Fragmentation-needed – The packet has the Don't Fragment bit set in the IP Flag field, but the HP device cannot forward the packet without fragmenting it.
- Host – The destination network or sub-net of the packet is directly connected to the HP device, but the host specified in the destination IP address of the packet is not on the network.
- Network – The HP device cannot reach the network specified in the destination IP address of the packet.
- Port – The destination host does not have the destination TCP or UDP port specified in the packet. In this case, the host sends the ICMP Port Unreachable message to the HP device, which in turn sends the message to the host that sent the packet.
- Protocol – The TCP or UDP protocol on the destination host is not running. This message is different from the Port Unreachable message, which indicates that the protocol is running on the host but the requested protocol port is unavailable.
- Source-route-failure – The device received a source-routed packet but cannot locate the next-hop IP address indicated in the packet’s Source-Route option.

**Note**

Disabling an ICMP Unreachable message type does not change the HP device’s ability to forward packets. Disabling ICMP Unreachable messages prevents the device from generating or forwarding the Unreachable messages.

To disable all ICMP Unreachable messages, enter the following command:

```
HPswitch(config)# no ip icmp unreachable
```

**Syntax:** `[no] ip icmp unreachable`
Disabling ICMP Redirects

You can disable ICMP redirects on the HP routing switch. only on a global basis, for all the routing switch interfaces. To disable ICMP redirects globally, enter the following command at the global CONFIG level of the CLI:

HPswitch(config)# no ip icmp redirects

**Syntax:** [no] ip icmp redirects

---

**Configuring Static IP Routes**

The IP route table can receive routes from the following sources:

- Directly-connected networks – When you add an IP VLAN interface, the routing switch automatically creates a route for the network the interface is in.
- RIP – If RIP is enabled, the routing switch can learn about routes from the advertisements other RIP routers send to the routing switch. If the route has a lower administrative distance than any other routes from different sources to the same destination, the routing switch places the route in the IP route table.
- OSPF – See RIP, but substitute “OSPF” for “RIP”.
- Statically configured route – You can add routes directly to the route table. When you add a route to the IP route table, you are creating a static IP route. This section describes how to add static routes to the IP route table.
- Default network route – This is a specific static route that the routing switch uses if other routes to the destination are not available. See “Configuring the Default Route” on page 10-19.

**Static Route Types**

You can configure the following types of static IP routes:

- **Standard** – the static route consists of the destination network address and network mask, and the IP address of the next-hop gateway. You can configure multiple standard static routes with the same metric for load sharing or with different metrics to provide a primary route and backup routes.
IP Routing Features
Configuring Static IP Routes

- **Null (reject)** – the static route consists of the destination network address and network mask, and the `reject` parameter. Typically, the null route is configured as a backup route for discarding traffic if the primary route is unavailable.

**Static IP Route Parameters**

When you configure a static IP route, you must specify the following parameters:

- The IP address and network mask for the route's destination network.
- The route's path, which can be one of the following:
  - The IP address of a next-hop gateway
  - A "null" interface. The routing switch drops traffic forwarded to the null interface.

The routing switch also applies fixed (*non-configurable*) default values for the following routing parameters:

- **The route’s metric** – The value the routing switch uses when comparing this route to other routes in the IP route table to the same destination. The metric applies only to routes that the routing switch has already placed in the IP route table. The fixed metric for static IP routes is 1.

- **The route’s administrative distance** – The value that the routing switch uses to compare this route with routes from other route sources to the same destination before placing a route in the IP route table. This parameter does not apply to routes that are already in the IP route table. The fixed administrative distance for static IP routes is 1.

The fixed metric and administrative distance values ensure that the routing switch always prefers static IP routes over routes from other sources to the same destination.

**Static Route States Follow Port States**

IP static routes remain in the IP route table only so long as the next-hop gateway, port, or virtual interface used by the route is available. If the gateway or port becomes unavailable, the software removes the static route from the IP route table. If the gateway or port later becomes available again, the software adds the route back to the route table.

This feature allows the routing switch to adjust to changes in network topology. The routing switch does not continue trying to use routes on unavailable paths but instead uses routes only when their paths are available.
The following command configures a static route to 207.95.7.0, using 207.95.6.157 as the next-hop gateway.

HPswitch(config)# ip route 207.95.7.0/24 207.95.6.157

When you configure a static IP route, you specify the destination address for the route and the next-hop gateway or routing switch interface through which the routing switch can reach the route. The routing switch adds the route to the IP route table. In this case, Router A knows that 207.95.6.157 is reachable through port A2, and also assumes that local interfaces within that sub-net are on the same port. Router A deduces that IP interface 207.95.7.188 is also on port A2.

The software automatically removes a static IP route from the IP route table if the port used by that route becomes unavailable. When the port becomes available again, the software automatically re-adds the route to the IP route table.

Configuring a Static IP Route

To configure an IP static route with a destination address of 192.0.0.0 255.0.0.0 and a next-hop router IP address of 195.1.1.1, enter the following commands:

HPswitch(config)# ip route 192.0.0.0 255.0.0.0 195.1.1.1

**Syntax:** \( \text{ip route < dest-ip-addr>/< mask-bits > < next-hop-ip-addr >} \)

The <dest-ip-addr> is the route’s destination. The <dest-mask> is the network mask for the route’s destination IP address. Alternatively, you can specify the network mask information by entering a forward slash followed by the number of bits in the network mask. For example, you can enter 192.0.0.0 255.255.255.0 as 192.0.0.0/.24.

Configuring the Default Route

You can also assign the default router as the destination by entering 0.0.0.0 0.0.0.0.

Configuring a “Null” Route

You can configure the routing switch to drop IP packets to a specific network or host address by configuring a “null” (sometimes called “null0”) static route for the address. When the routing switch receives a packet destined for the address, the routing switch drops the packet instead of forwarding it.
To configure a null static route to drop packets destined for network 209.157.22.x, enter the following commands:

```
HPswitch(config)# ip route 209.157.22.0 255.255.255.0 reject
HPswitch(config)# write memory
```

**Syntax:** `ip route <ip-addr> <ip-mask> reject`

*or*

```
ip route <ip-addr>/<mask-bits> reject
```

The `<ip-addr>` parameter specifies the network or host address. The routing switch will drop packets that contain this address in the destination field instead of forwarding them.

The `<ip-mask>` parameter specifies the network mask. Ones are significant bits and zeros allow any value. For example, the mask 255.255.255.0 matches on all hosts within the Class C sub-net address specified by `<ip-addr>`. Alternatively, you can specify the number of bits in the network mask. For example, you can enter 209.157.22.0/24 instead of 209.157.22.0 255.255.255.0.

The `reject` parameter indicates that this is a null route. You must specify this parameter to make this a null route.
Configuring RIP

This section describes how to configure RIP on HP Series 5300XL Switches using the CLI interface.

To display RIP configuration information and statistics, see “Displaying RIP Information” on page 10-27.

Overview of RIP

Routing Information Protocol (RIP) is an IP route exchange protocol that uses a distance vector (a number representing distance) to measure the cost of a given route. The cost is a distance vector because the cost often is equivalent to the number of router hops between the HP routing switch and the destination network.

An HP routing switch can receive multiple paths to a destination. The software evaluates the paths, selects the best path, and saves the path in the IP route table as the route to the destination. Typically, the best path is the path with the fewest hops. A hop is another router through which packets must travel to reach the destination. If the HP routing switch receives a RIP update from another router that contains a path with fewer hops than the path stored in the HP routing switch's route table, the routing switch replaces the older route with the newer one. The routing switch then includes the new path in the updates it sends to other RIP routers, including HP routing switches.

RIP routers, including HP routing switches, also can modify a route's cost, generally by adding to it, to bias the selection of a route for a given destination. In this case, the actual number of router hops may be the same, but the route has an administratively higher cost and is thus less likely to be used than other, lower-cost routes. A RIP route can have a maximum cost of 15. Any destination with a higher cost is considered unreachable. Although limiting to larger networks, the low maximum hop count prevents endless loops in the network.

HP Series 5300XL Switches support the following RIP types:

- Version 1
- V1 compatible with V2
- Version 2 (the default)

**Note**

ICMP Host Unreachable Message for Undeliverable ARPs. If the routing switch receives an ARP request packet that it is unable to deliver to the final destination because of the ARP timeout and no ARP response is received (the routing switch knows of no route to the destination address), the routing switch sends an ICMP Host Unreachable message to the source.
RIP Parameters and Defaults

The following tables list the RIP parameters, their default values, and where to find configuration information.

RIP Global Parameters

Table 10-3 lists the global RIP parameters and their default values.

**Table 10-3. RIP Global Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP state</td>
<td>Routing Information Protocol V2-only.</td>
<td>Disabled</td>
</tr>
<tr>
<td>auto-summary</td>
<td>Enable/Disable advertisement of summarized routes.</td>
<td>Enabled</td>
</tr>
<tr>
<td>metric</td>
<td>Default metric for imported routes.</td>
<td>1</td>
</tr>
<tr>
<td>redistribution</td>
<td>RIP can redistribute static and connected routes. (RIP redistributes connected routes by default, when RIP is enabled.)</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

RIP Interface Parameters

Table 10-4 lists the VLAN interface RIP parameters and their default values.

**Note**

RIP interface configuration is performed on VLAN interfaces on the Series 5300XL Switches.

**Table 10-4. RIP Interface Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
</table>
| RIP version | The version of the protocol that is supported on the interface.  
The version can be one of the following:  
• Version 1 only  
• Version 2 only  
• Version 1 compatible with version 2 | V2-only   |
| metric    | A numeric cost the routing switch adds to RIP routes learned on the interface. This parameter applies only to RIP routes. | 1         |
IP Routing Features
Configuring RIP

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>The routes that a routing switch learns or advertises can be controlled.</td>
<td>The routing switch learns and advertises all RIP routes on all RIP interfaces</td>
</tr>
<tr>
<td>loop prevention</td>
<td>The method the routing switch uses to prevent routing loops caused by advertising a route on the same interface as the one on which the routing switch learned the route.</td>
<td>Poison reverse</td>
</tr>
<tr>
<td>• Split horizon</td>
<td>the routing switch does not advertise a route on the same interface as the one on which the routing switch learned the route.</td>
<td></td>
</tr>
<tr>
<td>• Poison reverse</td>
<td>the routing switch assigns a cost of 16 (&quot;infinite&quot; or &quot;unreachable&quot;) to a route before advertising it on the same interface as the one on which the routing switch learned the route.</td>
<td></td>
</tr>
<tr>
<td>receive</td>
<td>Define the RIP version for incoming packets</td>
<td>V2-only</td>
</tr>
<tr>
<td>send</td>
<td>Define the RIP version for outgoing packets</td>
<td>V2-only</td>
</tr>
</tbody>
</table>

Configuring RIP Parameters

Use the following procedures to configure RIP parameters on a system-wide and individual VLAN interface basis.

Enabling RIP

RIP is disabled by default. To enable it, use one of the following methods. When you enable RIP, the default RIP version is **RIPv2-only**. You can change the RIP version on an individual interface basis to **RIPv1** or **RIPv1-compatible-v2** if needed.

To enable RIP on a routing switch, enter the following commands:

```bash
HPswitch(config)# ip routing
HPswitch(config)# router rip
HPswitch(config-rip-router)# exit
HPswitch(config)# write memory
```

**Syntax:** [no] router rip
**IP Routing Features**

**Configuring RIP**

**Note**

IP routing must be enabled prior to enabling RIP. The first command in the sequence above enables IP routing on the Series 5300XL Switch.

**Changing the RIP Type on a VLAN Interface**

When you enable RIP on a VLAN interface, **RIPv2-only** is enabled by default. You can change the RIP type to one of the following on an individual VLAN interface basis:

- Version 1 only
- Version 2 only (the default)
- Version 1 - compatible - version 2

To change the RIP type supported on a VLAN interface, enter commands such as the following:

```
HPswitch(config)# vlan 1
HPswitch(vlan-1)# ip rip v1-only
HPswitch(vlan-1)# exit
HPswitch(config)# write memory
```

**Syntax:** `[no] ip rip < v1-only | v1-compatible-v2 | v2-only >`

**Changing the Cost of Routes Learned on a VLAN Interface**

By default, a Series 5300XL Switch interface increases the cost of a RIP route that is learned on the interface. The switch increases the cost by adding one to the route's metric before storing the route.

You can change the amount that an individual VLAN interface adds to the metric of RIP routes learned on the interface.

**Note**

RIP considers a route with a metric of 16 to be unreachable. Use this metric only if you do not want the route to be used. In fact, you can prevent the Series 5300XL Switch from using a specific interface for routes learned though that interface by setting its metric to 16.

To increase the cost a VLAN interface adds to RIP routes learned on that interface, enter commands such as the following:

```
HPswitch(config)# interface vlan 1
HPswitch(vlan-1)# ip rip metric 5
```
These commands configure vlan-1 to add 5 to the cost of each route learned on the interface.

**Syntax**: ip rip metric < 1-16 >

**Configuring RIP Redistribution**

You can configure the routing switch to redistribute connected and static routes into RIP. When you redistribute a route into RIP, the routing switch can use RIP to advertise the route to its RIP neighbors.

To configure redistribution, perform the following tasks:

1. Configure redistribution filters to permit or deny redistribution for a route based on the destination network address or interface. (optional)
2. Enable redistribution

**Define RIP Redistribution Filters**

Route redistribution imports and translates different protocol routes into a specified protocol type. On HP Series 5300XL Switches, redistribution is supported for static routes and directly connected routes only. Redistribution of any other routing protocol into RIP is not currently supported. When you configure redistribution for RIP, you can specify that static or connected routes are imported into RIP routes. Likewise, OSPF redistribution supports the import of static or connected routes into OSPF routes.

To configure for redistribution, define the redistribution tables with “restrict” redistribution filters. In the CLI, use the `restrict` command for RIP at the RIP router level.

**Note**

Do not enable redistribution until you have configured the redistribution filters. Otherwise, the network might get overloaded with routes that you did not intend to redistribute.

**Example**: To configure the switch to filter out redistribution of static or connected routes on network 10.0.0.0, enter the following commands:

```
HPswitch(config)# router rip
HPswitch(rip)# restrict 10.0.0.0 255.0.0.0
HPswitch(rip)# write memory
```

**Note**

The default configuration permits redistribution for all default connected routes only.
Syntax: restrict <ip-addr> <ip-mask> | <ip-addr>/<prefix length>

This command prevents any routes with a destination address that is included in the range specified by the address/mask pair from being redistributed by RIP.

Modify Default Metric for Redistribution

The default metric is a global parameter that specifies the cost applied to all RIP routes by default. The default value is 1. You can assign a cost from 1 – 15.

Example: To assign a default metric of 4 to all routes imported into RIP, enter the following commands:

HPswitch(config)# router rip
HPswitch(rip)# default-metric 4

Syntax: default-metric <value>

The <value> can be from 1 – 15. The default is 1.

Enable RIP Route Redistribution

Do not enable redistribution until you have configured the redistribution filters. Otherwise, the network might get overloaded with routes that you did not intend to redistribute.

To enable redistribution of connected and static IP routes into RIP, enter the following commands.

HPswitch(config)# router rip
HPswitch(rip)# redistribute connected
HPswitch(rip)# redistribute static
HPswitch(rip)# write memory

Syntax: [no] redistribute connected | static
Changing the Route Loop Prevention Method

RIP can use the following methods to prevent routing loops:

- **Split horizon** - the routing switch does not advertise a route on the same interface as the one on which the routing switch learned the route.

- **Poison reverse** - the routing switch assigns a cost of 16 (“infinity” or “unreachable”) to a route before advertising it on the same interface as the one on which the routing switch learned the route. This is the default.

These loop prevention methods are configurable on an individual VLAN interface basis.

**Note**

These methods are in addition to RIP's maximum valid route cost of 15.

**Poison reverse** is enabled by default. Disabling poison reverse causes the routing switch to revert to **Split horizon**. (Poison reverse is an extension of Split horizon.) To disable Poison reverse on an interface, and thereby enable Split horizon, enter the following:

```
HPswitch(config)# vlan 1
HPswitch(vlan-1)# no ip rip poison-reverse
```

**Syntax:** [no] ip rip poison-reverse

Entering the command without the “no” option will re-enable Poison reverse.

Displaying RIP Information

All RIP configuration and status information is shown by the CLI command `show ip rip` and options off that command. The following RIP information can be displayed:

<table>
<thead>
<tr>
<th>RIP Information Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information</td>
<td>10-28</td>
</tr>
<tr>
<td>Interface Information</td>
<td>10-30</td>
</tr>
<tr>
<td>Peer Information</td>
<td>10-31</td>
</tr>
<tr>
<td>Redistribute Information</td>
<td>10-33</td>
</tr>
<tr>
<td>Restrict Information</td>
<td>10-33</td>
</tr>
</tbody>
</table>
Displaying General RIP Information

To display general RIP information, enter the following CLI command at any context level:

```
HPswitch# show ip rip
```

The resulting display will appear similar to the following:

<table>
<thead>
<tr>
<th>RIP global parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP protocol</td>
</tr>
<tr>
<td>Auto-summary</td>
</tr>
<tr>
<td>Default Metric</td>
</tr>
<tr>
<td>Route changes</td>
</tr>
<tr>
<td>Queries</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RIP interface information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>100.1.0.1</td>
</tr>
<tr>
<td>100.2.0.1</td>
</tr>
<tr>
<td>100.3.0.1</td>
</tr>
<tr>
<td>100.4.0.1</td>
</tr>
<tr>
<td>100.10.0.1</td>
</tr>
<tr>
<td>100.11.0.1</td>
</tr>
<tr>
<td>100.12.0.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RIP peer information</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>-------------</td>
</tr>
</tbody>
</table>

The display is a summary of Global RIP information, information about interfaces with RIP enabled, and information about RIP peers. The following fields are displayed:

- **RIP protocol** – Status of the RIP protocol on the router. RIP must be enabled here and on the VLAN interface for RIP to be active. The default is **disabled**.
- **Auto-summary** – Status of Auto-summary for all interfaces running RIP. If auto-summary is enabled, then subnets will be summarized to a class network when advertising outside of the given network.
■ **Default Metric** – Sets the default metric for imported routes. This is the metric that will be advertised with the imported route to other RIP peers. A RIP metric is a measurement used to determine the 'best' path to network; 1 is the best, 15 is the worse, 16 is unreachable.

■ **Route changes** – The number of times RIP has modified the routing switch’s routing table.

■ **Queries** – The number of RIP queries that have been received by the routing switch.

■ **RIP Interface Information** – RIP information on the VLAN interfaces on which RIP is enabled.
  - **IP Address** – IP address of the VLAN interface running rip.
  - **Status** – Status of RIP on the VLAN interface.
  - **Send mode** – The format of the RIP updates: RIP 1, RIP 2, or RIP 2 version 1 compatible.
  - **Recv mode** – The Series 5300XL Switches can process RIP 1, RIP 2, or RIP 2 version 1 compatible update messages.
  - **Metric** – The path “cost”, a measurement used to determine the 'best' RIP route path; 1 is the best, 15 is the worse, 16 is unreachable.
  - **Auth** – RIP messages can be required to include an authentication key if enabled on the interface.

■ **RIP Peer Information** – RIP Peers are neighboring routers from which the routing switch has received RIP updates.
  - **IP Address** – IP address of the RIP neighbor.
  - **Bad routes** – The number of route entries which were not processed for any reason.
  - **Last update timeticks** – How many seconds have passed since we received an update from this neighbor.

**Syntax:** show ip rip
Displaying RIP Interface Information

To display RIP interface information, enter the following CLI command at any context level:

HPswitch# show ip rip interface

The resulting display will appear similar to the following:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Status</th>
<th>Send mode</th>
<th>Recv mode</th>
<th>Metric</th>
<th>Auth</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.1.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>1</td>
<td>none</td>
</tr>
<tr>
<td>100.2.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>1</td>
<td>none</td>
</tr>
<tr>
<td>100.3.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>1</td>
<td>none</td>
</tr>
<tr>
<td>100.4.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>1</td>
<td>none</td>
</tr>
</tbody>
</table>

See “RIP Interface Information” on the previous page for definitions of these fields.

You can also display the information for a single RIP VLAN interface, by specifying the VLAN ID for the interface, or specifying the IP address for the interface.

**Displaying RIP interface information by VLAN ID:** For example, to show the RIP interface information for VLAN 1000, enter the following command:

HPswitch# show ip rip interface vlan 1000

```
RIP interface information for VLAN 1000
IP Address : 120.1.1.1
Status      : enabled
Send mode   : V2-only
Recv mode   : V2-only
Metric      : 1
Auth        : none

Bad packets received : 0
Bad routes received : 0
Sent updates : 0
```
The information in this display includes the following fields, which are defined under “RIP Interface Information” on page 10-29: **IP Address**, **Status**, **Send mode**, **Recv mode**, **Metric**, and **Auth**.

The information also includes the following fields:

- **Bad packets received** – The number of packets that were received on this interface and were not processed for any reason.
- **Bad routes received** – The number of route entries that were received on this interface and were not processed for any reason.
- **Sent updates** – The number of RIP routing updates that have been sent on this interface.

**Displaying RIP interface information by IP Address:** For example, to show the RIP interface information for the interface with IP address 100.2.0.1, enter the following command:

```
HPswitch# show ip rip interface 100.2.0.1
```

<table>
<thead>
<tr>
<th>RIP interface information for 100.2.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address : 100.2.0.1</td>
</tr>
<tr>
<td>Status : enabled</td>
</tr>
<tr>
<td>Send mode : V2-only</td>
</tr>
<tr>
<td>Recv mode : V2-only</td>
</tr>
<tr>
<td>Metric : 1</td>
</tr>
<tr>
<td>Auth : none</td>
</tr>
<tr>
<td>Bad packets received : 0</td>
</tr>
<tr>
<td>Bad routes received : 0</td>
</tr>
<tr>
<td>Sent updates : 0</td>
</tr>
</tbody>
</table>

The information shown in this display has the same fields as for the display for a specific VLAN ID. See the previous page for the definitions of these fields.

**Syntax:** `show ip rip interface [ip-addr | vlan < vlan-id >]`

**Displaying RIP Peer Information**

To display RIP peer information, enter the following CLI command at any context level:

```
HPswitch# show ip rip peer
```
The resulting display will appear similar to the following:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Bad routes</th>
<th>Last update timeticks</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.1.0.100</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>100.2.0.100</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>100.3.0.100</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>100.10.0.100</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

This display lists all neighboring routers from which the routing switch has received RIP updates. The following fields are displayed:

- **IP Address** – IP address of the RIP peer neighbor.
- **Bad routes** – The number of route entries that were not processed for any reason.
- **Last update timeticks** – How many seconds have passed since the routing switch received an update from this peer neighbor.

**Displaying RIP information for a specific peer:** For example, to show the RIP peer information for the peer with IP address 100.1.0.100, enter the following command:

```
HPswitch# show ip rip peer 100.1.0.100
```

<table>
<thead>
<tr>
<th>IP Address : 100.1.0.100</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad routes : 0</td>
</tr>
<tr>
<td>Last update timeticks : 2</td>
</tr>
</tbody>
</table>

This display lists the following information for a specific RIP peer:

- **IP Address** – IP address of the RIP peer neighbor.
- **Bad routes** – The number of route entries which were not processed for any reason.
- **Last update timeticks** – How many seconds have passed since the routing switch received an update from this neighbor.
Displaying RIP Redistribution Information

To display RIP redistribution information, enter the following CLI command at any context level:

HPswitch# show ip rip redistribute

```
RIP redistributing
Route type Status
---------- --------
connected enabled
static enabled
```

RIP automatically redistributes connected routes which are configured on interfaces that are running RIP, and all routes that are learned via RIP. The `router rip redistribute` command, described on page 10-25, configures the routing switch to cause RIP to advertise connected routes that are not running RIP, and static routes. The display shows whether RIP redistribution is enabled or disabled for connected and static routes.

Displaying RIP Redistribution Filter (restrict) Information

To display RIP restrict filter information, enter the following CLI command at any context level:

HPswitch# show ip rip restrict

```
RIP restrict list
 IP Address Mask
--------------- ---------------
```

The display shows if any routes, identified by the IP Address and Mask fields are being restricted from redistribution. The restrict filters are configured by the `router rip restrict` command described on page 10-25.
Configuring OSPF

This section describes how to configure OSPF on HP Series 5300XL Switches using the CLI interface.

To display OSPF configuration information and statistics, see “Displaying OSPF Information” on page 10-53.

Overview of OSPF

OSPF is a link-state routing protocol. The protocol uses link-state advertisements (LSA) to update neighboring routers regarding its interfaces and information on those interfaces. The Series 5300XL Switch floods these LSAs to all neighboring routers to update them regarding the interfaces. Each router maintains an identical database that describes its area topology to help a router determine the shortest path between it and any neighboring router.

HP Series 5300XL Switches support the following types of LSAs, which are described in RFC 2328:

- Router link
- Network link
- Summary link
- Autonomous system (AS) summary link
- AS external link

OSPF is built upon a hierarchy of network components. The highest level of the hierarchy is the Autonomous System (AS). An autonomous system is defined as a number of networks, all of which share the same routing and administration characteristics.

An AS can be divided into multiple areas. Each area represents a collection of contiguous networks and hosts. Areas define the limit to which link-state advertisements are broadcast, thereby limiting the amount of flooding that occurs within the network. An area is represented in OSPF by either an IP address or a number.

You can further limit the broadcast area of flooding by defining an area range. The area range allows you to assign an aggregate value to a range of IP addresses. This aggregate value becomes the address that is advertised instead all of the individual addresses it represents being advertised. You can assign up to 8 ranges in an OSPF area.
An OSPF router can be a member of multiple areas. Routers with membership in multiple areas are known as **Area Border Routers (ABRs)**. Each ABR maintains a separate topological database for each area the router is in. Each topological database contains all of the LSA databases for each router within a given area. The routers within the same area have identical topological databases. The ABR is responsible for forwarding routing information or changes between its border areas.

An **Autonomous System Boundary Router (ASBR)** is a router that is running multiple protocols and serves as a gateway to routers outside an area and those operating with different protocols. The ASBR is able to import and translate different protocol routes into OSPF through a process known as **redistribution**. For more details on redistribution and configuration examples, see “Enabling Route Redistribution” on page 10-50.

### Designated Routers in Multi-Access Networks

In a network that has multiple routers attached, OSPF elects one router to serve as the designated router (DR) and another router on the segment to act as the backup designated router (BDR). This arrangement minimizes the amount of repetitive information that is forwarded on the network by forwarding all messages to the designated router and backup designated routers responsible for forwarding the updates throughout the network.

### Designated Router Election

In a network with no designated router and no backup designated router, the neighboring router with the highest priority is elected as the DR, and the router with the next largest priority is elected as the BDR.

If the DR goes off-line, the BDR automatically becomes the DR. The router with the next highest priority becomes the new BDR.

**Note**

Priority is a configurable option at the interface level. You can use this parameter to help bias one Series 5300XL Switch as the DR.

If two neighbors share the same priority, the router with the highest router ID is designated as the DR. The router with the next highest router ID is designated as the BDR.

**Note**

By default, the HP router ID is the lowest numbered IP address configured on the device. For more information or to change the router ID, see “Changing the Router ID” on page 10-10.
When multiple Series 5300XL Switches on the same network are declaring themselves as DRs, then both priority and router ID are used to select the designated router and backup designated routers.

When only one router on the network claims the DR role despite neighboring routers with higher priorities or router IDs, this router remains the DR. This is also true for BDRs.

The DR and BDR election process is performed when one of the following events occurs:

- an interface is in a waiting state and the wait time expires
- an interface is in a waiting state and a hello packet is received that addresses the BDR
- a change in the neighbor state occurs, such as:
  - a neighbor state transitions from 2 or higher
  - communication to a neighbor is lost
  - a neighbor declares itself to be the DR or BDR for the first time

**OSPF RFC 1583 and 2328 Compliance**

HP Series 5300XL Switches are configured, by default, to be compliant with the RFC 1583 OSPF V2 specification. HP Series 5300XL Switches can also be configured to operate with the latest OSPF standard, RFC 2328.

**Note**

For details on how to configure the system to operate with the RFC 2328, see “Configuring OSPF” on page 10-38.

**Reduction of Equivalent AS External LSAs**

An OSPF ASBR uses AS External link advertisements (AS External LSAs) to originate advertisements of a route to another routing domain, such as a RIP domain. The ASBR advertises the route to the external domain by flooding AS External LSAs to all the other OSPF routers (except those inside stub networks) within the local OSPF Autonomous System (AS).

In some cases, multiple ASBRs in an AS can originate equivalent LSAs. The LSAs are equivalent when they have the same cost, the same next hop, and the same destination. The HP switch optimizes OSPF by eliminating duplicate AS External LSAs in this case. The switch with the lower router ID flushes the duplicate External LSAs from its database and thus does not flood the duplicate External LSAs into the OSPF AS. AS External LSA reduction therefore reduces the size of the switch’s link state database.
This enhancement implements the portion of RFC 2328 that describes AS External LSA reduction. This enhancement is enabled by default, requires no configuration, and cannot be disabled.

OSPF eliminates duplicate AS External LSAs. When two or more HP Series 5300XL Switches configured as ASBRs have equal-cost routes to the same next-hop router in an external routing domain, the ASBR with the highest router ID floods the AS External LSAs for the external domain into the OSPF AS, while the other ASBRs flush the equivalent AS External LSAs from their databases. As a result, the overall volume of route advertisement traffic within the AS is reduced and the Series 5300 Switches that flush the duplicate AS External LSAs have more memory for other OSPF data.

**Algorithm for AS External LSA Reduction.** The AS External LSA reduction feature behavior changes under the following conditions:

- There is one ASBR advertising (originating) a route to the external destination, but one of the following happens:
  - A second ASBR comes on-line
  - A second ASBR that is already on-line begins advertising an equivalent route to the same destination.

  In either case above, the Series 5300XL Switch with the higher router ID floods the AS External LSAs and the other Series 5300XL Switch flushes its equivalent AS External LSAs.

- One of the ASBRs starts advertising a route that is no longer equivalent to the route the other ASBR is advertising. In this case, the ASBRs each flood AS External LSAs. Since the LSAs either no longer have the same cost or no longer have the same next-hop router, the LSAs are no longer equivalent, and the LSA reduction feature no longer applies.

- The ASBR with the higher router ID becomes unavailable or is reconfigured so that it is no longer an ASBR. In this case, the other ASBR floods the AS External LSAs.
Dynamic OSPF Activation and Configuration

OSPF is automatically activated when you enable it. The protocol does not require a software reload.

Without ever having to reset the switch, you can change and save all the OSPF configuration options, including the following:

- all OSPF interface-related parameters (for example: area, hello timer, router dead time cost, priority, re-transmission time, transit delay)
- all area parameters
- all area range parameters
- all virtual-link parameters
- all global parameters
- creation and deletion of an area, interface or virtual link
- changes to address ranges
- changes to global values for redistribution
- addition of new virtual links

The only configuration change that requires you to disable and then re-enable OSPF operation is reconfiguring the Router ID.

Configuring OSPF

To begin using OSPF on the Series 5300XL Switch, perform the steps outlined below:

1. Enable routing on the routing switch.
2. Enable OSPF on the routing switch.
3. Assign the areas to which the routing switch will be attached.
4. Assign individual VLAN interfaces to the OSPF areas.
5. Define redistribution “restrict” filters, if desired.
6. Enable redistribution, if you defined redistribution filters.
7. Modify default global and interface parameters as required.
8. Modify OSPF standard compliance, if desired.

Note

OSPF is automatically enabled without a system reset.
Configuration Rules

- If a Series 5300 Switch is to operate as an ASBR, you must enable redistribution. When you do that, ASBR capability is automatically enabled.
- All Series 5300 Switch VLAN interfaces on which you wish to run OSPF must be assigned to one of the defined areas. When a VLAN interface is assigned to an area, the primary IP address is automatically included in the assignment. To include secondary addresses, you must enable OSPF on them separately, or use the “all” option in the assignment.

OSPF Parameters

You can modify or set the following global and interface OSPF parameters.

**Global Parameters:**
- Modify OSPF standard compliance setting.
- Assign an area.
- Define an area range.
- Define the area virtual link.
- Set global default metric for OSPF.
- Define redistribution metric type.
- Enable redistribution.
- Define redistribution restrict filters.
- Modify OSPF Traps generated.

**Interface Parameters:**
- Assign interfaces to an area.
- Select the authentication method (simple password or MD5) and the authentication key for the interface.
- Modify the cost for a link.
- Modify the dead interval.
- Modify the priority of the interface.
- Modify the retransmit interval for the interface.
- Modify the transit delay of the interface.
When using the CLI, you set global level parameters at the OSPF CONFIG Level of the CLI. To reach that level, make sure routing is enabled and then enter the command `router ospf` at the global CONFIG Level. Interface parameters for OSPF are set at the VLAN CONFIG Level using the CLI command `ip ospf`.

### Enabling OSPF on the Series 5300XL Switch

When you enable OSPF on the Series 5300XL Switch, the protocol is automatically activated. To enable OSPF on the Series 5300XL Switch, use the CLI commands:

```
HPswitch(config)# ip routing
HPswitch(config)# router ospf
```

The first command enables routing on the Series 5300XL Switch. The second command launches you into the OSPF router level where you can assign areas and modify OSPF global parameters.

### Regarding Disabling OSPF

Regarding Disabling OSPF. If you disable OSPF, the Series 5300XL Switch retains all the configuration information for the disabled protocol in flash memory. If you subsequently restart OSPF, that previous configuration will be applied.

### Assigning OSPF Areas

Assigning OSPF Areas

Once OSPF is enabled on the system, you can assign areas. Assign an IP address or number as the **area ID** for each area. The area ID is representative of only the primary IP address. To include secondary addresses, you must enable OSPF on them separately, or use the “all” option in the assignment. Each VLAN interface on a Series 5300XL switch can support 16 areas.

You can assign subnets individually to areas. The limit on the number of areas is 16.

An area can be **normal** or a **stub**.

- **Normal** – Series 5300XL Switches within an OSPF normal area can send and receive External Link State Advertisements (LSAs).
Stub – Series 5300XL Switches within an OSPF stub area cannot send or receive External LSAs. In addition, the routing switches in an OSPF stub area must use a default route to the area's Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) to send traffic out of the area.

Example: Here is an example of the commands to set up several OSPF areas.

HPswitch(ospf)# area 192.5.1.0
HPswitch(ospf)# area 200.5.0.0
HPswitch(ospf)# area 0.0.0.0
HPswitch(ospf)# write memory

Syntax: area <num> | <ip-addr> [normal | stub <cost> [no-summary]]

The <num> | <ip-addr> parameter specifies the area number, which can be a number or in IP address format. If you specify a number, the number can be from 0 – 4,294,967,295.

The <cost> specifies the cost of the default route to be injected into the stub area, if this routing switch is an ABR. The value can be from 1 – 16,777,215. If you configure a stub area, you must specify the cost. There is no default. Normal areas do not use the cost parameter.

Note

The switch CLI requires that you enter a cost value when specifying the stub parameter, but this cost value is ignored. The actual cost is provided by the Area Border Router (ABR).

The no-summary parameter applies only to stub areas and disables summary LSAs from being sent into the area. See “Disabling Summary LSAs” below.

Disabling Summary LSAs

By default, the Series 5300XL Switch sends summary LSAs (LSA type 3) into stub areas. You can further reduce the number of LSAs sent into a stub area by configuring the Series 5300XL Switch to stop sending summary LSAs into the area. You can disable the summary LSAs when you are configuring the stub area or later after you have configured the area.

This feature disables origination of summary LSAs, but the Series 5300XL Switch still accepts summary LSAs from OSPF neighbors and floods them to other neighbors. The Series 5300XL Switch can form adjacencies with other routers regardless of whether summarization is enabled or disabled for areas on each Series 5300XL Switch.
When you enter a command to disable the summary LSAs, the change takes effect immediately. If you apply the option to a previously configured area, the Series 5300XL Switch flushes all of the summary LSAs it has generated (as an ABR) from the area.

**Note**

This feature applies only when the Series 5300XL Switch is configured as an Area Border Router (ABR) for the area. To completely prevent summary LSAs from being sent to the area, disable the summary LSAs on each OSPF router that is an ABR for the area.

To disable summary LSAs for a stub area, enter commands such as the following:

```
HPswitch(config-ospf-router)# area 40 stub 3 no-summary
```

### Assigning an Area Range (optional)

You can assign a range for an area, but it is not required. Ranges allow a specific IP address and mask to represent a range of IP addresses within an area, so that only that reference range address is advertised to the network, instead of all the addresses within that range. Each area can have up to 8 range addresses.

**Example.** To define an area range for sub-nets on 193.45.5.1 and 193.45.6.2, enter the following commands:

```
HPswitch(config)# router ospf
HPswitch(ospf)# area 192.45.5.1 range 193.45.0.0 255.255.0.0
HPswitch(ospf)# area 193.45.6.2 range 193.45.0.0 255.255.0.0
```

**Syntax:** area < ospf-area-id \| backbone > range < ip-addr/mask-length > [no-advertise]

The `<ospf-area-id>` parameter specifies the area number, which can be in IP address format.

The `<ip-addr>` parameter following `range` specifies the IP address portion of the range. The software compares the address with the significant bits in the mask. All network addresses that match this comparison are summarized in a single route advertised by the Series 5300XL Switch.
The `<mask-length>` parameter specifies the portions of the IP address that a route must contain to be summarized in the summary route. In the example above, all networks that begin with 209.157 are summarized into a single route.

Assigning VLANs to an Area

Once you define OSPF areas, you can assign VLANs to the areas. All Series 5300XL Switch VLANs must be assigned to one of the defined areas on an OSPF router. When a VLAN is assigned to an area, the primary IP address is automatically included in the assignment. To include secondary addresses, you must enable OSPF on them separately, or use the “all” option in the assignment.

**Example:** To assign VLAN 8 of Switch A to area 192.5.0.0 and then save the changes, enter the following commands:

```
HPSwitch(ospf)# vlan 8
RouterA(vlan-8)# ip ospf area 192.5.0.0
RouterA(vlan-8)# write memory
```

Modifying Interface Defaults

OSPF has interface parameters that you can configure. For simplicity, each of these parameters has a default value. No change to these default values is required except as needed for specific network configurations.

VLAN default values can be modified using the following CLI commands at the VLAN interface level of the CLI:

- `ip ospf area <ip-addr>`
- `ip ospf authentication-key <password>`
- `ip ospf md5-auth-key-chain <chain-name-str>`
- `ip ospf cost <num>`
- `ip ospf dead-interval <value>`
- `ip ospf hello-interval <value>`
- `ip ospf priority <value>`
- `ip ospf retransmit-interval <value>`
- `ip ospf transmit-delay <value>`

For a complete description of these parameters, see the summary of OSPF interface parameters in the next section.
OSPF Interface Parameters

The following parameters apply to OSPF interfaces.

**Area:** Assigns an interface to a specific area. You can assign either an IP address or number to represent an OSPF Area ID. If you assign a number, it can be any value from 0 – 4,294,967,295.

**Authentication-key:** OSPF supports two methods of authentication for each VLAN—simple password and MD5. In addition, the value can be set to none, meaning no authentication is performed. Only one method of authentication can be active on a subnet at a time. The default authentication value is none. The two authentication methods are configured by different commands:

- **Simple password** – Use the `ip ospf authentication-key <password>` command. The simple password method of authentication requires you to configure an alphanumeric password on an interface. The simple password setting takes effect immediately. All OSPF packets transmitted on the interface contain this password. Any OSPF packet that is received on the interface is checked for this password. If the password is not present, then the packet is dropped. The password can be up to eight characters long.

- **MD5** – Use the `ip ospf md5-auth-key-chain <chain-name-str>` command. The MD5 method of authentication uses key chains that you configure through the Key Management System (KMS – described in your switch Security Guide). The `<chain-name-str>` is the name of the key chain that you have previously configured by using the KMS commands.

**Cost:** Indicates the overhead required to send a packet across an interface. You can modify the cost to differentiate between 100 Mbps and 1000 Mbps (1 Gbps) links. The default cost is always 1.

**Dead-interval:** Indicates the number of seconds that a neighbor router waits for a hello packet from the current Series 5300XL Switch before declaring the Series 5300XL Switch down. The value can be from 1 – 2,147,483,647 seconds. The default is 40 seconds.

**Hello-interval:** Represents the length of time between the transmission of hello packets. The value can be from 1 – 65535 seconds. The default is 10 seconds.

**Priority:** Allows you to modify the priority of an OSPF router. The priority is used when selecting the designated router (DR) and backup designated routers (BDRs). The value can be from 0 – 255. The default is 1. If you set the priority to 0, the Series 5300XL Switch does not participate in DR and BDR election.
**Retransmit-interval**: The time between retransmissions of link-state advertisements (LSAs) to adjacent routers for this interface. The value can be from 0 – 3600 seconds. The default is 5 seconds.

**Transit-delay**: The time it takes to transmit Link State Update packets on this interface. The value can be from 0 – 3600 seconds. The default is 1 second.

**Assigning Virtual Links**

It is highly recommended that all ABRs (area border routers) have either a direct or indirect link to the OSPF backbone area (0.0.0.0 or 0). If an ABR does not have a physical link to the area backbone, the ABR can configure a virtual link to another router within the same area, which has a physical connection to the area backbone.

*Note*

A backbone area can be purely virtual with no physical backbone links. Also note that virtual links can be “daisy chained”. If so, it may not have one end physically connected to the backbone.

The path for a virtual link is through an area shared by the neighbor ABR (router with a physical backbone connection), and the ABR requiring a logical connection to the backbone.

Two parameters must be defined for all virtual links—**transit area ID** and **neighbor router**.

- The **transit area ID** represents the shared area of the two ABRs and serves as the connection point between the two routers. This number should match the area ID value.
- The **neighbor router** field is the router ID (IP address) of the router that is physically connected to the backbone, when assigned from the router interface requiring a logical connection. When assigning the parameters from the router with the physical connection, the router ID is the IP address of the router requiring a logical connection to the backbone.

*Note*

By default, the HP router ID is the lowest numbered IP address configured on the device. For more information or to change the router ID, see “Changing the Router ID” on page 10-10.

*Note*

When you establish an area virtual link, you must configure it on both of the routers (both ends of the virtual link).
Example. Figure 10-1 shows an OSPF area border router, Routing Switch-A, that is cut off from the backbone area (Area 0). To provide backbone access to Routing Switch-A, you can add a virtual link between Routing Switch-A and Routing Switch-C using Area 1 as a transit area. To configure the virtual link, you define the link on the router that is at each end of the link. No configuration for the virtual link is required on the routers in the transit area.

To configure the virtual link on Routing Switch-A, enter the following commands:

```
HPswitch(ospf)# area 1 virtual-link 209.157.22.1
HPswitch(ospf)# write memory
```
To configure the virtual link on Routing Switch-C, enter the following commands:

HPswitch(ospf)# area 1 virtual-link 10.0.0.1
HPswitch(ospf)# write memory

Syntax: area <ip-addr> | <num> virtual-link <router-id>

The area < ip-addr > | < num > parameter specifies the transit area.

The <router-id> parameter specifies the router ID of the OSPF router at the remote end of the virtual link. To display the router ID on an HP Series 5300XL Switch, enter the show ip command.

See “Modify Virtual Link Parameters” below for descriptions of the optional parameters.

Modifying Virtual Link Parameters

OSPF has some parameters that you can modify for virtual links. Notice that these are a subset of the parameters that you can modify for physical interfaces. **cost** is not configured for virtual links, it is calculated by route calculation.

You can modify default values for virtual links using the following CLI command at the **OSPF router level** of the CLI, as shown in the following syntax:

Syntax: area < num > | < ip-addr > virtual-link < ip-addr > [authentication-key < string >| md5-auth-key-chain < chain-name-str >] [dead-interval < num >] [hello-interval < num >] [retransmit-interval < num >] [transmit-delay < num >]

The parameters are described below. For syntax information, at the CLI prompt, enter the command **area help**.

Virtual Link Parameter Descriptions

You can modify the following virtual link interface parameters:

**Authentication Key**: OSPF supports two methods of authentication for each virtual link—**simple password** and **MD5**. In addition, the value can be set to **none**, meaning no authentication is performed. Only one method of authentication can be active on a subnet at a time. The default authentication value is none. The two authentication methods are configured by different commands:
**Simple password** – Use the `area <num> | <ip-addr> virtual-link <ip-addr> authentication-key <password>` command. The simple password method of authentication requires you to configure an alphanumeric password on an interface. The simple password setting takes effect immediately. All OSPF packets transmitted on the interface contain this password. Any OSPF packet that is received on the interface is checked for this password. If the password is not present, then the packet is dropped. The password can be up to eight characters long.

**MD5** – Use the `area <num> | <ip-addr> virtual-link <ip-addr> md5-auth-key-chain <name>` command. The MD5 method of authentication uses key chains that you configure through the Key Management System (KMS – described in your switch Security Guide). The `<name>` is the name of the key chain that you have previously configured by using the KMS commands.

**Hello Interval**: The length of time between the transmission of hello packets. The range is 1 – 65535 seconds. The default is 10 seconds.

**Retransmit Interval**: The interval between the re-transmission of link state advertisements to router adjacencies for this interface. The range is 0 – 3600 seconds. The default is 5 seconds.

**Transmit Delay**: The period of time it takes to transmit Link State Update packets on the interface. The range is 0 – 3600 seconds. The default is 1 second.

**Dead Interval**: The number of seconds that a neighbor router waits for a hello packet from the current routing switch before declaring the routing switch down. The range is 1 – 65535 seconds. The default is 40 seconds.

**Defining Redistribution Filters**

Route redistribution imports and translates different protocol routes into a specified protocol type. On HP Series 5300XL Switches, redistribution is supported for only static routes and directly connected routes. Redistribution of any other routing protocol into OSPF is not currently supported. When you configure redistribution for OSPF, you can specify that static or connected routes are imported into OSPF routes. Likewise, RIP redistribution supports the import of static or connected routes into RIP routes.

To configure for redistribution, define the redistribution tables with restrict redistribution filters. In the CLI, use the `restrict` command for OSPF at the OSPF router level.
Do not enable redistribution until you have configured the redistribution filters. Otherwise, the network might get overloaded with routes that you did not intend to redistribute.

**Example:** To configure the Series 5300XL Switch acting as an ASBR to filter out redistribution of static or connected routes on network 10.0.0.0, enter the following commands:

```plaintext
HPswitchASBR(config)# router ospf
HPswitch(ospf)# restrict 10.0.0.0 255.0.0.0
HPswitch(ospf)# write memory
```

**Note**

Redistribution is permitted for all routes by default.

**Syntax:** `restrict <ip-addr> <ip-mask> | <ip-addr>/<prefix length>`

This command prevents any routes with a destination address that is included in the range specified by the address/mask pair from being redistributed by OSPF.

**Modifying Default Metric for Redistribution**

The default metric is a global parameter that specifies the cost applied to all OSPF routes by default. The default value is 10. You can assign a cost from 1 – 16,777,215.

**Example:** To assign a default metric of 4 to all routes imported into OSPF, enter the following commands:

```plaintext
HPswitch(config)# router ospf
HPswitch(ospf)# default-metric 4
```

**Syntax:** `default-metric <value>`

The `<value>` can be from 1 – 16,777,215. The default is 10.
Enabling Route Redistribution

**Note**

Do not enable redistribution until you have configured the redistribution “restrict” filters. Otherwise, the network might get overloaded with routes that you did not intend to redistribute.

To enable redistribution of connected and static IP routes into OSPF, enter the following commands.

```
HPswitch(config)# router ospf
HPswitch(ospf)# redistribution connected
HPswitch(ospf)# redistribution static
HPswitch(ospf)# write memory
```

**Syntax:** [no] redistribution connected | static

**Modifying Redistribution Metric Type**

The redistribution metric type is used by default for all routes imported into OSPF. Type 1 metrics are the same “units” as internal OSPF metrics and can be compared directly. Type 2 metrics are not directly comparable, and are treated as larger than the largest internal OSPF metric. The default value is type 2.

To modify the default value to type 1, enter the following command:

```
HPswitch(config-ospf-router)# metric-type type1
```

**Syntax:** metric-type type1 | type2

The default is type2.

**Administrative Distance**

HP Series 5300XL Switches can learn about networks from various protocols, including RIP, and OSPF. Consequently, the routes to a network may differ depending on the protocol from which the routes were learned. For the Series 5300XL Switches, the administrative distance for OSPF routes is set at 110.

The Series 5300XL Switch selects one route over another based on the source of the route information. To do so, the Series 5300XL Switch can use the administrative distances assigned to the sources.
Modifying OSPF Traps Generated

OSPF traps as defined by RFC 1850 are supported on HP Series 5300XL Switches. OSPF trap generation is enabled on the Series 5300XL Switch, by default.

When using the CLI, you can disable all or specific OSPF trap generation by entering the following CLI command:

```
HPswitch(ospf)# no snmp-server trap ospf
```

To later re-enable the trap feature, enter the command:

```
HPswitch(ospf)# snmp-server trap ospf
```

To disable a specific OSPF trap, enter the following command:

```
HPswitch(ospf)# no snmp-server trap ospf < ospf-trap >.
```

These commands are at the OSPF Router Level of the CLI.

Here is a summary of OSPF traps supported on HP Series 5300XL Switches, and their associated MIB objects from RFC 1850:

**Table 10-5. OSPF Traps and Associated MIB Objects**

<table>
<thead>
<tr>
<th>OSPF Trap Name</th>
<th>MIB Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-state-change-trap</td>
<td>ospflfstateChange</td>
</tr>
<tr>
<td>virtual-interface-state-change-trap</td>
<td>ospfvirtlfStateChange</td>
</tr>
<tr>
<td>neighbor-state-change-trap</td>
<td>ospfvirtNbrStateChange</td>
</tr>
<tr>
<td>virtual-neighbor-state-change-trap</td>
<td>ospfvirtNbrStateChange</td>
</tr>
<tr>
<td>interface-config-error-trap</td>
<td>ospflfConfigError</td>
</tr>
<tr>
<td>virtual-interface-config-error-trap</td>
<td>ospfvirtlfConfigError</td>
</tr>
<tr>
<td>interface-authentication-failure-trap</td>
<td>ospflfAuthFailure</td>
</tr>
<tr>
<td>virtual-interface-authentication-failure-trap</td>
<td>ospfvirtlfAuthFailure</td>
</tr>
<tr>
<td>interface-receive-bad-packet-trap</td>
<td>ospflfrxBadPacket</td>
</tr>
<tr>
<td>virtual-interface-receive-bad-packet-trap</td>
<td>ospfvirtlfRxBadPacket</td>
</tr>
<tr>
<td>interface-retransmit-packet-trap</td>
<td>ospftxRetransmit</td>
</tr>
<tr>
<td>virtual-interface-retransmit-packet-trap</td>
<td>ospfvirtlfTxRetransmit</td>
</tr>
</tbody>
</table>
**OSPF Trap Name** | **MIB Object**
--- | ---
origin-lsa-trap | ospfOriginateLsa
origin-maxage-lsa-trap | ospfMaxAgeLsa
link-state-database-overflow-trap | ospfLsdbOverflow
link-state-database-approaching-overflow-trap | ospfLsdbApproachingOverflow

**Examples:**

1. To stop an OSPF trap from being collected, use the following CLI command:

   ```
   HPswitch(ospf)# no trap < ospf-trap >
   ```

2. To disable reporting of the neighbor-state-change-trap, enter the following command:

   ```
   HPswitch(ospf)# no trap neighbor-state-change-trap
   ```

3. To reinstate the trap, enter the following command:

   ```
   HPswitch(ospf)# trap neighbor-state-change-trap
   ```

**Syntax:** `[no] snmp-server trap ospf < ospf-trap >`

**Modifying OSPF Standard Compliance Setting**

**Note**

All routes in an AS should be configured with the same compliance setting. If any routers in a domain support only RFC 1583, then all routers must be configured with 1583 compatibility.

If all the routers support RFC 2178 or RFC 2328, you should disable RFC 1583 compatibility on all the routers in the domain, since these standards are more robust against routing loops on external routes.

HP Series 5300XL Switches are configured, by default, to be compliant with the RFC 1583 OSPF V2 specification.

To configure a Series 5300XL Switch to operate with the latest OSPF standard, RFC 2328, enter the following commands:

```
HPswitch(config)# router ospf
HPswitch(ospf)# no rfc1583-compatibility
```

**Syntax:** `[no] rfc1583-compatibility`
Displaying OSPF Information

You can use CLI commands to display the following OSPF information:

<table>
<thead>
<tr>
<th>OSPF Information Type</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information</td>
<td>10-53</td>
</tr>
<tr>
<td>Area information</td>
<td>10-55</td>
</tr>
<tr>
<td>External link state information</td>
<td>10-56</td>
</tr>
<tr>
<td>Interface information</td>
<td>10-57</td>
</tr>
<tr>
<td>Link state information</td>
<td>10-60</td>
</tr>
<tr>
<td>Neighbor information</td>
<td>10-62</td>
</tr>
<tr>
<td>Route information</td>
<td>10-68</td>
</tr>
<tr>
<td>Virtual Neighbor information</td>
<td>10-65</td>
</tr>
<tr>
<td>Virtual Link information</td>
<td>10-66</td>
</tr>
</tbody>
</table>

Displaying General OSPF Configuration Information

To display general OSPF configuration information, enter the following command at any CLI level:

HPswitch# show ip ospf general

OSPF General Status

OSPF protocol : enabled
Router ID : 10.0.8.36
RFC 1583 compatibility : compatible

Default import metric : 1
Default import metric type : external type 2

Area Border : yes
AS Border : yes
External LSA Count : 9
External LSA Checksum Sum : 408218
Originate New LSA Count : 24814
Receive New LSA Count : 14889
**Syntax:** show ip ospf general

The following fields are shown in the OSPF general status display:

**Table 10-6. CLI Display of OSPF General Information**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF protocol</td>
<td>indicates whether OSPF is currently enabled.</td>
</tr>
<tr>
<td>Router ID</td>
<td>the Router ID that this routing switch is currently using to identify itself</td>
</tr>
<tr>
<td>RFC 1583 compatibility</td>
<td>indicates whether the routing switch is currently using RFC 1583 (compatible) or RFC 2328 (non-compatible rules for calculating external routes.</td>
</tr>
<tr>
<td>Default import metric</td>
<td>indicates the default metric that will be used for any routes redistributed into OSPF by this routing switch</td>
</tr>
<tr>
<td>Default import metric type</td>
<td>indicates the metric type (type 1 or type 2) that will be used for any routes redistributed into OSPF by this routing switch</td>
</tr>
<tr>
<td>Area Border</td>
<td>indicates whether this routing switch is currently acting as an area border router</td>
</tr>
<tr>
<td>AS Border</td>
<td>indicates whether this routing switch is currently acting as an autonomous system border router (redistributing routes)</td>
</tr>
<tr>
<td>External LSA Count</td>
<td>indicates the total number of external LSAs currently in the routing switch’s link state database</td>
</tr>
<tr>
<td>External LSA Checksum Sum</td>
<td>the sum of the checksums of all external LSAs currently in the routing switch’s link state database (quick check for whether database is in sync with other routers in the routing domain)</td>
</tr>
<tr>
<td>Originate New LSA Count</td>
<td>count of the number of times this switch has originated a new LSA</td>
</tr>
<tr>
<td>Receive New LSA Count</td>
<td>count of the number of times this switch has received a new LSA</td>
</tr>
</tbody>
</table>
Displaying OSPF Area Information

To display OSPF area information, enter the following command at any CLI level:

```
HPswitch> show ip ospf area
```

<table>
<thead>
<tr>
<th>OSPF Area Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>0.0.0.0</td>
</tr>
<tr>
<td>192.147.60.0</td>
</tr>
<tr>
<td>192.147.80.0</td>
</tr>
</tbody>
</table>

**Syntax:** show ip ospf area [ospf-area-id]

The [ospf-area-id] parameter shows information for the specified area. If no area is specified, information for all the OSPF areas configured is displayed.

The OSPF area display shows the following information:

<table>
<thead>
<tr>
<th><strong>Table 10-7. CLI Display of OSPF Area Information</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>This Field...</strong></td>
</tr>
<tr>
<td>Area ID</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>normal</td>
</tr>
<tr>
<td>stub</td>
</tr>
<tr>
<td>Cost</td>
</tr>
<tr>
<td>SPFR</td>
</tr>
<tr>
<td>ABR</td>
</tr>
<tr>
<td>ASBR</td>
</tr>
<tr>
<td>LSA</td>
</tr>
<tr>
<td>Chksum(Hex)</td>
</tr>
</tbody>
</table>
Displaying OSPF External Link State Information

To display external link state information, enter the following command at any CLI level:

```
HPswitch# show ip ospf external-link-state
```

When you enter this command, an output similar to the following is displayed:

<table>
<thead>
<tr>
<th>Link State ID</th>
<th>Router ID</th>
<th>Age</th>
<th>Sequence #</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.7.0</td>
<td>10.0.8.37</td>
<td>232</td>
<td>0x80000005</td>
<td>0x0000c3b3</td>
</tr>
<tr>
<td>10.3.8.0</td>
<td>10.0.8.37</td>
<td>232</td>
<td>0x80000005</td>
<td>0x0000cea9</td>
</tr>
<tr>
<td>10.3.9.0</td>
<td>10.0.8.37</td>
<td>232</td>
<td>0x80000005</td>
<td>0x0000c3b3</td>
</tr>
<tr>
<td>10.3.10.0</td>
<td>10.0.8.37</td>
<td>232</td>
<td>0x80000005</td>
<td>0x0000b8bd</td>
</tr>
<tr>
<td>10.3.33.0</td>
<td>10.0.8.36</td>
<td>1098</td>
<td>0x80000005</td>
<td>0x0000b8bd</td>
</tr>
</tbody>
</table>

**Syntax:** `show ip ospf external-link-state`

The OSPF external link state display shows the following information:

**Table 10-8. CLI Display of OSPF External Link State Information**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link State ID</td>
<td>LSA ID for this LSA. Normally, the destination of the external route, but may have some “host” bits set.</td>
</tr>
<tr>
<td>Router ID</td>
<td>Router ID of the router that originated this external LSA.</td>
</tr>
<tr>
<td>Age</td>
<td>Current age (in seconds) of this LSA.</td>
</tr>
<tr>
<td>Sequence #</td>
<td>Sequence number of the current instance of this LSA.</td>
</tr>
<tr>
<td>Chksum(Hex)</td>
<td>LSA checksum value.</td>
</tr>
</tbody>
</table>

**Syntax:** `show ip ospf external-link-state [status | advertise] [link-state-id < link-state-id> | router-id < router-id> | sequence-number < sequence#>]`

The **status** keyword is optional and can be omitted. The output can be filtered to show a subset of the total output by specifying the **link-state-id**, **router-id**, or **sequence-number** options.

The **advertise** keyword displays the hexadecimal data in the specified LSA packet, the actual contents of the LSAs. This can also be filtered as above by including the **link-state-id**, **router-id**, or **sequence-number** options.
An example of the **show ip ospf external-link-state advertise** is the following:

<table>
<thead>
<tr>
<th>OSPF External LSAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertisements</td>
</tr>
<tr>
<td>000302050a307000a008258000005d99f0024fffff008000000a0000000000000000</td>
</tr>
<tr>
<td>000302050a308000a00082580000005cea90024fffff008000000a0000000000000000</td>
</tr>
<tr>
<td>000302050a309000a00825800000005c3b0024fffff008000000a0000000000000000</td>
</tr>
<tr>
<td>000302050a30a000a0082580000005b8bd0024fffff008000000a0000000000000000</td>
</tr>
<tr>
<td>000002050a321000a00824800009c0930024fffff00800000010000000000000000</td>
</tr>
</tbody>
</table>

### Displaying OSPF Interface Information

To display OSPF interface information, enter the following command at any CLI level:

```
HPswitch# show ip ospf interface
```

<table>
<thead>
<tr>
<th>OSPF Interface Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>10.3.18.36</td>
</tr>
<tr>
<td>10.3.53.36</td>
</tr>
</tbody>
</table>

**Syntax:** show ip ospf interface [vlan <vlan-id> | <ip-addr>]

The OSPF interface display shows the following information:

**Table 10-9. CLI Display of OSPF Interface Information**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The local IP address for this interface.</td>
</tr>
<tr>
<td>Status</td>
<td>enabled or disabled - whether OSPF is currently enabled on this interface.</td>
</tr>
<tr>
<td>Area ID</td>
<td>The ID of the area that this interface is in.</td>
</tr>
</tbody>
</table>
### IP Routing Features

**Configuring OSPF**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
</table>
| **State**     | The current state of the interface. The value will be one of the following:  
|               | • DOWN - the underlying VLAN is down  
|               | • WAIT - the underlying VLAN is up, but we are waiting to hear hellos from other routers on this interface before we run designated router election  
|               | • DR - this switch is the designated router for this interface  
|               | • BDR - this switch is the backup designated router for this interface  
|               | • DROTHER - this router is not the designated router or backup designated router for this interface |
| **Auth-type** | none or simple - will be none if no authentication key is configured, simple if an authentication key is configured. All routers running OSPF on the same link must be using the same authentication type and key. |
| **Cost**      | The OSPF's metric for this interface. |
| **Priority**  | This routing switch’s priority on this interface for use in the designated router election algorithm. |

The `<ip-addr>` parameter displays the OSPF interface information for the specified IP address.

### Displaying OSPF Interface Information for a Specific VLAN or IP Address

To display OSPF interface information for a specific VLAN or IP address, enter a command such as the following at any CLI level:

```
HPswitch# show ip ospf interface 10.3.18.36
```
**IP Routing Features**

**Configuring OSPF**

<table>
<thead>
<tr>
<th>OSPF Interface Status for 10.3.18.36</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address : 10.3.18.36 Status : enabled</td>
</tr>
<tr>
<td>Area ID : 10.3.16.0</td>
</tr>
<tr>
<td>State : BDR Auth-type : none</td>
</tr>
<tr>
<td>Cost : 1 Priority : 1</td>
</tr>
<tr>
<td>Type : BCAST</td>
</tr>
<tr>
<td>Transit Delay : 1 Retrans Interval : 5</td>
</tr>
<tr>
<td>Hello Interval : 10 Rtr Dead Interval : 40</td>
</tr>
<tr>
<td>Designated Router : 10.3.18.34 Events : 3</td>
</tr>
<tr>
<td>Backup Desig. Rtr : 10.3.18.36</td>
</tr>
</tbody>
</table>

**Syntax:** show ip ospf interface [vlan <vlan-id> | <ip-addr>]

The OSPF interface display for a specific VLAN or IP address has the same information as the non-specific show ip ospf interface command for the IP Address, Area ID, Status, State, Auth-type, Cost, and Priority fields. See the information for the general command above for definitions of these fields.

The show ip ospf interface command for a specific VLAN or IP address shows the following additional information:

**Table 10-10. CLI Display of OSPF Interface Information – VLAN or IP Address**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Will always be <strong>BCAST</strong> for interfaces on this routing switch. Point-to-point or NBMA (frame relay or ATM) type interfaces are not supported on HP Procurve Series 5300XL Switches.</td>
</tr>
<tr>
<td>Transit Delay</td>
<td>Configured transit delay for this interface.</td>
</tr>
<tr>
<td>Retrans Interval</td>
<td>Configured retransmit interval for this interface.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>Configured hello interval for this interface.</td>
</tr>
<tr>
<td>Rtr Dead Interval</td>
<td>Configured router dead interval for this interface.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>IP address of the router that has been elected designated router on this interface.</td>
</tr>
<tr>
<td>Backup Desig. Rtr</td>
<td>IP address of the router that has been elected backup designated router on this interface.</td>
</tr>
</tbody>
</table>
IP Routing Features
Configuring OSPF

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>Number of times the interface state has changed.</td>
</tr>
</tbody>
</table>

If you issue a `show ip ospf interface vlan <vlan-id>` command, the information will be the same as shown in the previous table, but for the primary IP address on the indicated VLAN.

Displaying OSPF Link State Information

To display OSPF link state information, enter the following command at any CLI level:

```
HPswitch# show ip ospf link-state
```

When you enter this command, an output similar to the following is displayed:

```
OSPF Link State Database for Area 0.0.0.0
Advertising
LSA Type Link State ID Router ID Age Sequence # Checksum
---------- --------------- --------------- ---- ... 10.3.17.0 10.0.8.35 1316 0x80000002 0x00002cba
AsbSummary 10.0.8.34 10.0.8.34 1735 0x80000005 0x00001465
```

Syntax: `show ip ospf link-state`

The OSPF link state display shows contents of the LSA database, one table for each area. The following information is shown:
Table 10-11. CLI Display of OSPF Link State Information

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSA Type</td>
<td>Type of LSA. The possible types are: Router Network Summary AsbSummary</td>
</tr>
<tr>
<td>Link State ID</td>
<td>LSA ID for this LSA. The meaning depends on the LSA type.</td>
</tr>
<tr>
<td>Advertised Router ID</td>
<td>Router ID of the router that originated this LSA.</td>
</tr>
<tr>
<td>Age</td>
<td>Current age (in seconds) of this LSA.</td>
</tr>
<tr>
<td>Sequence #</td>
<td>Sequence number of the current instance of this LSA.</td>
</tr>
<tr>
<td>Chksum(Hex)</td>
<td>LSA checksum value.</td>
</tr>
</tbody>
</table>

Other options for this command: The status keyword is optional and can be omitted. The output can be filtered to show a subset of the total output by specifying the area-id, link-state-id, router-id, LSA type, or sequence-number options.

The advertise keyword displays the hexadecimal data in the specified LSA packet, the actual contents of the LSAs. This can also be filtered as above by including the area-id, link-state-id, router-id, LSA type, or sequence-number options.

The full syntax of the command is as follows:

Syntax: show ip ospf link-state [status | advertise] [< area-id > | link-state-id < link-state-id > | router-id < router-id > | type < router | network | summary | as-summary > | sequence-number < sequence# >]
An example of the `show ip ospf link-state advertise` is the following:

```
OSPF Link State Database for Area 0.0.0.0
Advertisements
---------------------------------------------
000202010a000820800000281a7b6005400000050a30e00fffff00300001...
000202010a0008210a00082180000006a5c90024010000010a0008230a03112104000002
000102010a0008230a00082380000015755d006c010000070a030600fffff003000001...
000202020a0302250a000825800000702440024fffff000a0008250a0008230a000820
000202030a0310000a00082180000008c043001cfffff00000000002
000102030a0310000a00082380000009a85901cfffff000000000001
000002030a0310000a00082480000009ac53001cfffff000000000002
000202040a0008240a000821800000032abb001c000000000000000b
000102040a0008240a00082380000004c12a001c0000000000000002

OSPF Link State Database for Area 10.3.16.0
Advertisements
---------------------------------------------
000202010a0008210a000821800000027fd33d0054050000050a31900fffff003000001...
000102010a0008220a000822800000284dc5000600000060a031500fffff003000001...
000102020a0311220a00082280000027bf9080020fffff000a0008220a000821
```

Displaying OSPF Neighbor Information

To display OSPF neighbor information, enter the following command at any CLI level:

```
HPswitch(ospf)# show ip ospf neighbor
```

```
OSPF Neighbor Information
 Router ID  Pri IP Address NbIfState State Rxmt QLen Events
----------- ----------------- --------- ------ --------- ----------
10.0.8.34   1  10.3.18.34   DR       FULL     0        6
10.3.53.38  1  10.3.53.38   DR       FULL     0        6
```

**Syntax:** `show ip ospf neighbor [ ip-addr ]`

The `[ip-addr]` can be specified to retrieve detailed information for the specific neighbor only. This is the IP address of the neighbor, not the Router ID.
This display shows the following information.

**Table 10-12. CLI Display of OSPF Neighbor Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The router ID of the neighbor.</td>
</tr>
<tr>
<td>Pri</td>
<td>The OSPF priority of the neighbor. The priority is used during election of the Designated Router (DR) and Backup designated Router (BDR).</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of this routing switch’s interface with the neighbor.</td>
</tr>
<tr>
<td>NbIfState</td>
<td>The neighbor interface state. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• DR – this neighbor is the elected designated router for the interface.</td>
</tr>
<tr>
<td></td>
<td>• BDR – this neighbor is the elected backup designated router for the interface.</td>
</tr>
<tr>
<td></td>
<td>• blank – this neighbor is neither the DR or the BDR for the interface.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the conversation (the adjacency) between your routing switch and the neighbor. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• INIT – A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor. (The Series 5300XL Switch itself did not appear in the neighbor’s Hello packet.) All neighbors in this state (or higher) are listed in the Hello packets sent from the associated interface.</td>
</tr>
<tr>
<td></td>
<td>• 2WAY – Communication between the two routers is bidirectional. This is the most advanced state before beginning adjacency establishment. The Designated Router and Backup Designated Router are selected from the set of neighbors in the 2Way state or greater.</td>
</tr>
<tr>
<td></td>
<td>• EXSTART – The first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial Database Description (DD) sequence number. Neighbor conversations in this state or greater are called adjacencies.</td>
</tr>
<tr>
<td></td>
<td>• EXCHANGE – The Series 5300XL Switch is describing its entire link state database by sending Database Description packets to the neighbor. Each Database Description packet has a DD sequence number, and is explicitly acknowledged. Only one Database Description packet can be outstanding at any time. In this state, Link State Request packets can also be sent asking for the neighbor’s more recent advertisements. All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets.</td>
</tr>
<tr>
<td></td>
<td>• LOADING – Link State Request packets are sent to the neighbor asking for the more recent advertisements that have been discovered (but not yet received) in the Exchange state.</td>
</tr>
<tr>
<td></td>
<td>• FULL – The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network link advertisements.</td>
</tr>
<tr>
<td>Rxmt QLen</td>
<td>Remote transmit queue length – the number of LSAs that the routing switch has sent to this neighbor and for which the routing switch is awaiting acknowledgements.</td>
</tr>
<tr>
<td>Events</td>
<td>The number of times the neighbor’s state has changed.</td>
</tr>
</tbody>
</table>
Displaying OSFPF Redistribution Information

As described under “Enabling Route Redistribution” on page 10-50, you can configure the routing switch to redistribute connected and static routes into OSPF. When you redistribute a route into OSPF, the routing switch can use OSPF to advertise the route to its OSPF neighbors.

To display the status of the OSPF redistribution, enter the following command at any CLI context level:

```
HPswitch# show ip ospf redistribute
```

<table>
<thead>
<tr>
<th>OSPF redistributing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route type</td>
</tr>
<tr>
<td>-------------</td>
</tr>
<tr>
<td>connected</td>
</tr>
<tr>
<td>static</td>
</tr>
</tbody>
</table>

The display shows whether redistribution of each of the route types, connected and static is enabled.

Displaying OSFPF Redistribution Filter (restrict) Information

As described under “Defining Redistribution Filters” on page 10-48, you can configure the redistribution filters on the routing switch to restrict route redistribution by OSPF.

To display the status of the OSPF redistribution filters, enter the following command at any CLI context level:

```
HPswitch# show ip ospf restrict
```

<table>
<thead>
<tr>
<th>OSPF restrict list</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td>10.0.8.0</td>
</tr>
<tr>
<td>15.0.0.0</td>
</tr>
</tbody>
</table>

This display shows the configured restrict entries.
Displaying OSPF Virtual Neighbor Information

To display OSPF virtual neighbor information, enter the following command at any CLI level:

```
HPswitch# show ip ospf virtual-neighbor
```

<table>
<thead>
<tr>
<th>OSPF Virtual Interface Neighbor Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td>10.0.8.33</td>
</tr>
<tr>
<td>10.0.8.36</td>
</tr>
</tbody>
</table>

**Syntax:** `show ip ospf virtual-neighbor [area < area-id > | < ip-address >]`

This display shows the following information.

**Table 10-13. CLI Display of OSPF Virtual Neighbor Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router ID</td>
<td>The router ID of this virtual neighbor (configured).</td>
</tr>
<tr>
<td>Area ID</td>
<td>The area ID of the transit area for the virtual link to this neighbor (configured).</td>
</tr>
<tr>
<td>State</td>
<td>The state of the adjacency with this virtual neighbor. The possible values are the same as the OSPF neighbor states. See the State parameter definition in table 10-12 on page 10-63. Note that virtual neighbors should never stay in the 2WAY state.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the virtual neighbor that the routing switch is using to communicate to that virtual neighbor.</td>
</tr>
<tr>
<td>Events</td>
<td>The number of times the virtual neighbor’s state has changed.</td>
</tr>
</tbody>
</table>

Notice from the syntax statement that you can get OSPF virtual neighbor information for a specific area or a specific IP address.
Displaying OSPF Virtual Link Information

To display OSPF virtual link information, enter the following command at any CLI level:

HPswitch# show ip ospf virtual-link

<table>
<thead>
<tr>
<th>Transit AreaID</th>
<th>Neighbor Router</th>
<th>Authentication</th>
<th>Interface State</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.16.0</td>
<td>10.0.8.33</td>
<td>none</td>
<td>P2P</td>
</tr>
<tr>
<td>10.3.16.0</td>
<td>10.0.8.36</td>
<td>none</td>
<td>P2P</td>
</tr>
</tbody>
</table>

**Syntax:** show ip ospf virtual-link [area < area-id | ip-address ]

This display shows the following information.

**Table 10-14. CLI Display of OSPF Virtual Link Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit Area ID</td>
<td>Area ID of transit area for the virtual link.</td>
</tr>
<tr>
<td>Neighbor Router</td>
<td>Router ID of the virtual neighbor.</td>
</tr>
<tr>
<td>Authentication</td>
<td>none or simple (same as for normal interface).</td>
</tr>
<tr>
<td>Interface State</td>
<td>The state of the virtual link to the virtual neighbor. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• DOWN – the routing switch has not yet found a route to the virtual neighbor.</td>
</tr>
<tr>
<td></td>
<td>• P2P – (point-to-point) the routing switch has found a route to the virtual neighbor. Virtual links are “virtual” serial links, hence the point-to-point terminology.</td>
</tr>
</tbody>
</table>

Notice from the syntax statement that you can get OSPF virtual link information for a specific area or a specific IP address.

**Example:** To get OSPF virtual link information for IP address 10.0.8.33, enter the command:

HPswitch# show ip ospf virtual-link 10.0.8.33

A display similar to the following is shown.
OSPF Virtual Interface Status for interface 10.0.8.33

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transit AreaID</td>
<td>10.3.16.0</td>
</tr>
<tr>
<td>Neighbor Router</td>
<td>10.0.8.33</td>
</tr>
<tr>
<td>Authentication</td>
<td>none</td>
</tr>
<tr>
<td>Transit Delay</td>
<td>1</td>
</tr>
<tr>
<td>Interface State</td>
<td>P2P</td>
</tr>
<tr>
<td>Rtr Interval</td>
<td>5</td>
</tr>
<tr>
<td>Events</td>
<td>1</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>10</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>40</td>
</tr>
</tbody>
</table>

Events

The number of times the virtual link interface state has changed.

Transit delay

The configured transit delay for the virtual link.

Rtr Interval

The configured retransmit interval for the virtual link.

Hello Interval

The configured hello interval for the virtual link.

Dead Interval

The configured router dead interval for the virtual link.
Displaying OSPF Route Information

To display OSPF route and other OSPF configuration information, enter the following command at any CLI level:

```
HPswitch# show ip ospf
```

### OSPF Configuration Information

- **OSPF protocol**: enabled
- **Router ID**: 10.0.8.35

**Currently defined areas:**

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Stub Type</th>
<th>Default Cost</th>
<th>Stub Summary LSA</th>
<th>Stub Metric Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>backbone</td>
<td>normal 1</td>
<td></td>
<td>don't send</td>
<td>ospf metric</td>
</tr>
<tr>
<td>10.3.16.0</td>
<td>normal 1</td>
<td></td>
<td>don't send</td>
<td>ospf metric</td>
</tr>
<tr>
<td>10.3.32.0</td>
<td>normal 1</td>
<td></td>
<td>don't send</td>
<td>ospf metric</td>
</tr>
</tbody>
</table>

**Currently defined address ranges:**

<table>
<thead>
<tr>
<th>Area ID</th>
<th>LSA Type</th>
<th>IP Network</th>
<th>Network Mask</th>
<th>Advertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.16.0</td>
<td>Summary</td>
<td>10.3.16.0</td>
<td>255.255.255.0</td>
<td>yes</td>
</tr>
</tbody>
</table>

**OSPF interface configuration:**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Area ID</th>
<th>Admin Status</th>
<th>Authen Type</th>
<th>Cost</th>
<th>Pri</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.2.35</td>
<td>backbone</td>
<td>enabled</td>
<td>BCAST none</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.3.3.35</td>
<td>backbone</td>
<td>enabled</td>
<td>BCAST none</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.3.16.35</td>
<td>10.3.16.0</td>
<td>enabled</td>
<td>BCAST none</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.3.32.35</td>
<td>10.3.32.0</td>
<td>enabled</td>
<td>BCAST none</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**OSPF configured interface timers:**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Transit Delay</th>
<th>Retransmit Interval</th>
<th>Hello Interval</th>
<th>Dead Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.2.35</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>10.3.3.35</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>10.3.16.35</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>10.3.32.35</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
</tbody>
</table>

**OSPF configured virtual interfaces:**

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Router ID</th>
<th>Authen Type</th>
<th>Xmit Delay</th>
<th>Rxmt Intvl</th>
<th>Hello Intvl</th>
<th>Dead Intvl</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.16.0</td>
<td>10.0.8.33</td>
<td>none</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td>10.3.16.0</td>
<td>10.0.8.36</td>
<td>none</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>40</td>
</tr>
</tbody>
</table>
**Syntax:** `show ip ospf`

This screen has a lot of information, most of it already covered in other `show` commands. The following table shows definitions for the fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF protocol</td>
<td><em>enabled</em> or <em>disabled</em> – indicates if OSPF is currently enabled.</td>
</tr>
<tr>
<td>Router ID</td>
<td>The Router ID that this routing switch is currently using to identify itself.</td>
</tr>
</tbody>
</table>

**Currently Defined Areas:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>The identifier for this area.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of OSPF area (normal or stub).</td>
</tr>
<tr>
<td>Stub Default Cost</td>
<td>The metric for any default route we will inject into a stub area if we are an ABR for the area.</td>
</tr>
<tr>
<td>Stub Summary LSA</td>
<td><em>send</em> or <em>don’t send</em> – indicates the state of the no-summary option for the stub area. The value indicates if the area is “totally stubby” (no summaries sent from other areas) or just “stub” (summaries sent). Only applies to stub areas, and only takes effect if the routing switch is the ABR for the area.</td>
</tr>
<tr>
<td>Stub Metric Type</td>
<td>This value is always <em>ospf metric</em>.</td>
</tr>
</tbody>
</table>

**Currently defined address ranges:**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>The area where the address range is configured.</td>
</tr>
<tr>
<td>LSA Type</td>
<td>This value is always <em>Summary</em>.</td>
</tr>
<tr>
<td>IP Network</td>
<td>The address part of the address range specification.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>The mask part of the address range specification.</td>
</tr>
<tr>
<td>Advertise</td>
<td>Whether we are advertising <em>(yes)</em> or suppressing <em>(no)</em> this address range.</td>
</tr>
</tbody>
</table>

**Note**

The remaining interface and virtual link information is the same as for the previously described OSPF show commands.
Configuring IRDP

The ICMP Router Discovery Protocol (IRDP) is used by HP routing switches to advertise the IP addresses of its router interfaces to directly attached hosts. IRDP is enabled by default. You can enable the feature on a global basis or on an individual VLAN interface basis.

When IRDP is enabled, the routing switch periodically sends Router Advertisement messages out the IP interfaces on which the feature is enabled. The messages advertise the routing switch's IP addresses to directly attached hosts who listen for the messages. In addition, hosts can be configured to query the routing switch for the information by sending Router Solicitation messages.

Some types of hosts use the Router Solicitation messages to discover their default gateway. When IRDP is enabled on the HP routing switch, the routing switch responds to the Router Solicitation messages. Some clients interpret this response to mean that the routing switch is the default gateway. If another router is actually the default gateway for these clients, leave IRDP disabled on the HP routing switch.

IRDP uses the following parameters. If you enable IRDP on individual VLAN interfaces, you can configure these parameters on an individual VLAN interface basis.

- **Packet type** - The routing switch can send Router Advertisement messages as IP broadcasts or as IP multicasts addressed to IP multicast group 224.0.0.1. The default packet type is IP broadcast.

- **Hold time** - Each Router Advertisement message contains a hold time value. This value specifies the maximum amount of time the host should consider an advertisement to be valid until a newer advertisement arrives. When a new advertisement arrives, the hold time is reset. The hold time is always longer than the maximum advertisement interval. Therefore, if the hold time for an advertisement expires, the host can reasonably conclude that the router interface that sent the advertisement is no longer available. The default hold time is three times the maximum message interval.

- **Maximum message interval and minimum message interval** - When IRDP is enabled, the routing switch sends the Router Advertisement messages every 450-600 seconds by default. The time within this interval that the routing switch selects is random for each message and is not affected by traffic loads or other network factors. The random interval minimizes the probability that a host will receive Router Advertisement
messages from other routers at the same time. The interval on each IRDP-enabled routing switch interface is independent of the interval on other IRDP-enabled interfaces. The default maximum message interval is 600 seconds. The default minimum message interval is 450 seconds.

- **Preference** - If a host receives multiple Router Advertisement messages from different routers, the host selects the router that send the message with the highest preference as the default gateway. The preference can be a number from -4294967296 to 4294967295. The default is 0.

### Enabling IRDP Globally

To enable IRDP globally, enter the following command:

```
HP(config)# ip irdp
```

This command enables IRDP on the IP interfaces on all ports. Each port uses the default values for the IRDP parameters.

### Enabling IRDP on an Individual VLAN Interface

To enable IRDP on an individual VLAN interface and configure IRDP parameters, enter commands such as the following:

```
HP(config)# vlan 1
HP(vlan-1)# ip irdp maxadvertinterval 400
```

This example shows how to enable IRDP on a specific interface (VLAN 1) and change the maximum advertisement interval for Router Advertisement messages to 400 seconds.

**Syntax:**
```
[no] ip irdp [broadcast | multicast] [holdtime <seconds>] [maxadvertinterval <seconds>] [minadvertinterval <seconds>] [preference <number>]
```

- **broadcast | multicast** - This parameter specifies the packet type the routing switch uses to send the Router Advertisement.
  - **broadcast** - The routing switch sends Router Advertisements as IP broadcasts.
  - **multicast** - The routing switch sends Router Advertisements as multicast packets addressed to IP multicast group 224.0.0.1. This is the default.
- **holdtime <seconds>** - This parameter specifies how long a host that receives a Router Advertisement from the routing switch should consider the advertisement to be valid. When a host receives a new Router Advertisement message from the routing switch, the host resets the hold time
for the routing switch to the hold time specified in the new advertisement. If the hold time of an advertisement expires, the host discards the advertisement, concluding that the router interface that sent the advertisement is no longer available. The value must be greater than the value of the maxadvertinterval parameter and cannot be greater than 9000. The default is three times the value of the maxadvertinterval parameter.

- **maxadvertinterval** - This parameter specifies the maximum amount of time the routing switch waits between sending Router Advertisements. You can specify a value from 1 to the current value of the holdtime parameter. The default is 600 seconds.

- **minadvertinterval** - This parameter specifies the minimum amount of time the routing switch can wait between sending Router Advertisements. The default is three-fourths (0.75) the value of the maxadvertinterval parameter. If you change the maxadvertinterval parameter, the software automatically adjusts the minadvertinterval parameter to be three-fourths the new value of the maxadvertinterval parameter. If you want to override the automatically configured value, you can specify an interval from 1 to the current value of the maxadvertinterval parameter.

- **preference <number>** - This parameter specifies the IRDP preference level of this routing switch. If a host receives Router Advertisements from multiple routers, the host selects the router interface that sent the message with the highest preference as the host's default gateway. The valid range is -4294967296 to 4294967295. The default is 0.

### Displaying IRDP Information

To display IRDP information, enter the following command from any CLI level:

`HPswitch# show ip irdp`

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Advertising Address</th>
<th>Min int (sec)</th>
<th>Max int (sec)</th>
<th>Holdtime (sec)</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT_VLAN</td>
<td>Enabled</td>
<td>multicast</td>
<td>450</td>
<td>600</td>
<td>1800</td>
<td>0</td>
</tr>
<tr>
<td>VLAN20</td>
<td>Enabled</td>
<td>multicast</td>
<td>450</td>
<td>600</td>
<td>1800</td>
<td>0</td>
</tr>
<tr>
<td>VLAN30</td>
<td>Enabled</td>
<td>multicast</td>
<td>450</td>
<td>600</td>
<td>1800</td>
<td>0</td>
</tr>
</tbody>
</table>
Configuring DHCP Relay

Overview

The Dynamic Host Configuration Protocol (DHCP) is used for configuring hosts with IP address and other configuration parameters without human intervention. The protocol is composed of three components: the DHCP client, the DHCP server, and the DHCP relay agent. The DHCP client sends broadcast request packets to the network, the DHCP servers respond with broadcast packets that offer IP parameters, such as an IP address for the client. After the client chooses the IP parameters, communication between the client and server is by unicast packets.

The function of the DHCP relay agent is to forward the DHCP messages to other subnets so that the DHCP server doesn’t have to be on the same subnet as the DHCP clients. The DHCP relay agent transfers the DHCP messages from DHCP clients located on a subnet without DHCP server, to other subnets. It also relays answers from DHCP servers to DHCP clients.

DHCP Packet Forwarding

The DHCP relay agent on the routing switch forwards DHCP client packets to all DHCP servers that are configured in the table administrated for each VLAN.

Unicast Forwarding

The packets are forwarded using unicast forwarding if the IP address of the DHCP server is a specific host address. The DHCP relay agent sets the destination IP address of the packet to the IP address of the DHCP server and forwards the message.

Broadcast Forwarding

The packets are forwarded using broadcast forwarding if the IP address of the DHCP server is a subnet address or IP broadcast address (255.255.255.255). The DHCP relay agent sets the DHCP server IP address will be set to broadcast IP address and forwarded to all VLANs with configured IP interfaces (except the source VLAN).
Minimum Requirements for DHCP Relay Operation

In order for the DHCP Relay agent to work, the following steps must be completed:

1. DHCP Relay is enabled on the routing switch (the default setting)
2. A DHCP server is servicing the routing switch
3. IP Routing is enabled on the routing switch
4. There is a route from the DHCP server to the routing switch and back
5. An IP Helper address is configured on the routing switch, set to the IP address of the DHCP server on the VLAN that is connected to the DHCP Client.

Enabling DHCP Relay

The factory-default configuration enables DHCP. However, if DHCP has been disabled, you can re-enable it at the Config CLI context level by entering this command:

```plaintext
HPswitch(config)# dhcp-relay
```

To disable the DHCP Relay function, enter the command:

```plaintext
HPswitch(config)# no dhcp-relay
```

Configuring a Helper Address

At the VLAN configuration CLI context level, enter the commands to add the DHCP server’s IP address to the VLANs list. For example, to configure a helper address for VLAN 1, enter these commands:

```plaintext
HPswitch(conf)# vlan 1
HPswitch(vlan-1)# ip helper-address <ip-addr>
```

To remove the DHCP server helper address, enter this command:

```plaintext
HPswitch(vlan-1)# no ip helper-address <ip-addr>
```
Viewing the Current DHCP Relay Configuration

**Determining the DHCP Relay Setting.** Use `show config` (or `show running` for the running-config file) to list the current DHCP Relay setting. Note that because DHCP Relay is enabled in the default configuration, it does not appear in these listings unless it is disabled.

```bash
HPswitch(config)# show config
Startup configuration:
; J4850A Configuration Editor; Created on release E.07.21
hostname "HPswitch"
cdp run
module 1 type J4820A
ip default-gateway 18.30.240.1
snmp-server community "public" Unrestricted
vlan 1
  name "DEFAULT_VLAN"
  untagged A1
  ip address 18.30.240.180 255.255.248.0
  no untagged A2-A24
exit
no dhcp-relay  Non-Default DHCP-Relay Setting
```

**Figure 10-2. Example of Startup-Config Listing with DHCP-Relay Disabled**

**Listing the Currently Configured DHCP Helper Addresses.**

**Syntax:** `show ip helper-address < vlan-id >`

This command shows the currently configured IP Helper addresses, regardless of whether DHCP-Relay is enabled. For example:

```bash
HPswitch(config)# show ip helper-address vlan 1
IP Helper Addresses
  IP Helper Address
  ----------
  10.28.227.97
  10.29.227.53
```

**Figure 10-3. Example of Listing for IP Helper Addresses**
Configuring Static Network Address Translation (NAT) for Intranet Applications

Static NAT is useful in applications where you want to conceal a “private”, or hidden region of your network from the general population of users in the “public” region, but allow access from the “public” region to selected devices in the hidden region. NAT performs this function by translating the IP addresses of the selected devices so that they appear to logically reside in the public region of your network instead of in a hidden region. This is done by mapping a virtual, public IP address to the actual, private IP address of the device you want to make accessible to clients in the public region. For example:

<table>
<thead>
<tr>
<th>Client Name</th>
<th>IP Seen in Corporate (Public) Region:</th>
<th>Configured (Private) IP:</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>15.33.235.10</td>
<td>10.10.10.11</td>
</tr>
<tr>
<td>B</td>
<td>15.33.235.32</td>
<td>10.10.10.12</td>
</tr>
<tr>
<td>C</td>
<td>15.33.235.38</td>
<td>10.10.10.13</td>
</tr>
</tbody>
</table>

Figure 10-4. Example of a Static NAT Application in an Intranet

Static NAT operates globally, on a per-switch basis and evaluates all incoming and outgoing packets on all ports. NAT performs IP address mapping only on packets having a source or destination IP address appearing in the static NAT table the switch maintains when NAT is configured. Note also that static NAT operates at the layer 3 level. IP addresses embedded in layers 4 - 7, as is the case with some applications, are not translated by static NAT.
Static NAT Operating Rules

- Uses one-to-one IP address mapping. That is, with each “private” device IP address you configure for static NAT, there must be a corresponding virtual, “public” IP address.
- Allows up to 32 client IP addresses per switch, which requires an equal number of virtual IP address assignments. Note that increasing the number of NAT mappings can reduce overall NAT performance.
- Requires routing to be enabled on the switch.

Configuring Static NAT

Syntax:  

[no] ip nat static <private-ip> <public-ip>

Configures the switch to map a virtual IP address over the actual IP address for a device residing in a region of your network that is hidden from general network users.

<private-ip>: This is the IP address of a device in a region of your network that you want to remain hidden from general network users. (This address is the actual IP address configured on the device.)

<public-ip>: This is the virtual IP address you want to use to access (from the public region of the network) a specific device residing in the hidden portion of the network.

With NAT configured, the switch intercepts the traffic requesting the <public-ip> address and redirects it to the corresponding <private-ip> address. In this case, the switch translates the destination ip address to the <private-ip> address and then forwards the traffic normally. In the opposite direction, the switch intercepts the traffic from a configured <private-ip> address destined to the public network and translates the <private-ip> address to its corresponding <public-ip> address before forwarding the traffic.

You can configure up to 32 IP NAT static mappings on the switch, which means you can map the configured IP addresses of 32 devices to corresponding virtual IP addresses. The [no] form of the command removes the specified static NAT assignment from the switch’s running configuration.
**Example.** This example uses the topology in figure 10-4 on page 10-76:

- The switch is connected to the corporate intranet through VLAN 100 (IP address: 15.33.235.1).
- The three devices are configured on VLAN 101 in the corporation’s “private” region (IP address: 10.10.10.1) with these IP addresses:
  A. 10.10.10.11
  B. 10.10.10.12
  C. 10.10.10.13
- The system administrator selects these virtual IP addresses to make the three devices appear to reside in the corporation’s “public” region:
  A. 15.33.235.10
  B. 15.33.235.32
  C. 15.33.235.38

To configure the static NAT mapping between the actual IP addresses configured on the devices and the corresponding virtual IP addresses:

```
HPswitch(config)# ip nat static 10.10.10.11 15.33.235.10
HPswitch(config)# ip nat static 10.10.10.12 15.33.235.32
HPswitch(config)# ip nat static 10.10.10.13 15.33.235.38
```

The above commands create the virtual IP address mappings in figure 10-5:

![Figure 10-5. Example of Static NAT Mapping of Virtual IP Addressing](image-url)
Displaying Static NAT Statistics and Configuration

**Syntax:** show ip nat

Displays the current IP NAT static configuration in the running-config file and the current IP NAT counters.

**Total Translations:** Displays a 32-bit counter showing the number of packets in which IP NAT has translated the source or destination IP address from a private address to a public address or from a public address to a private address.

For example, the following shows a sample of `show ip nat` output for the example on page 10-78.

```
HPswitch# show ip nat
Total translations: 26784

<table>
<thead>
<tr>
<th>Private</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.11</td>
<td>15.33.235.10</td>
</tr>
<tr>
<td>10.10.10.12</td>
<td>15.33.235.32</td>
</tr>
<tr>
<td>10.10.10.13</td>
<td>15.33.235.38</td>
</tr>
</tbody>
</table>
```

**Figure 10-6. Example of Displaying NAT Mappings**

**Static NAT Operating Notes**

- Static NAT on the 5300XL switches is a method for accessing a private region within an intranet. It is not the dynamic NAT often used for IP address translation from private IP addresses to registered, global IP addresses on the internet, and is not supported for Internet NAT applications.

- Non-NAT hosts in the same subnet (VLAN) as NAT hosts will be routed normally. That is, the IP addresses of hosts without a static NAT entry will not be translated.

- Static NAT is not intended for bandwidth-intensive or high-traffic applications, and such environments can degrade NAT performance.

- For a given virtual IP address, static NAT applies the subnet mask that is configured in the corresponding actual IP addressing.

- Static NAT does not provide TCP/UDP port number translation.

- Static NAT is not intended to support a large number of clients.

- Static NAT is not a security application and should not be considered as a substitute for a firewall.
Router Redundancy Using XRRP

Contents

Introduction to XRRP .................................................. 11-2
Terminology ............................................................... 11-2
Overview of XRRP Operation ....................................... 11-3
  XRRP During Normal Router Operation ....................... 11-4
  XRRP Fail-Over Operation ......................................... 11-5
    Single VLAN Operation ........................................... 11-5
    Multiple VLAN Operation ....................................... 11-6
  XRRP Operation Notes ............................................. 11-9
Configuring XRRP ...................................................... 11-11
  Customizing the XRRP Configuration .......................... 11-12
  Enabling and Disabling XRRP .................................... 11-15
  Configuration Rules ............................................... 11-15
  Configuration Examples ......................................... 11-16
    Configuration for Figure 11-2 – Single VLAN Example . 11-16
    Configuration for Figure 11-4 – Multiple VLANs .......... 11-17
Displaying XRRP Data ................................................. 11-18
Comparison Between XRRP and VRRP ............................. 11-21
Introduction to XRRP

XRRP (XL Router Redundancy Protocol) is the feature used by the HP Procurve Series 5300XL switches to provide router redundancy, or fail-over, to a backup router in case one fails. XRRP is similar to the industry standard VRRP (Virtual Router Redundancy Protocol), although the details of the operation are different.

Throughout this discussion, the 5300XL switches are considered as routers and the term “router” is used to identify them.

Terminology

The following terms are used in the description of XRRP:

- **Protection Domain** – A pair of physical routers that are running XRRP and are configured to provide fail-over protection for each other.

- **Virtual Router** – A virtual routing device that provides a router interface to host computers that are accessing it. Each physical router in the Protection Domain can own a virtual router. On fail-over, one physical router may own all the virtual routers in the Protection Domain. Movement of the virtual router responsibility, as part of the XRRP operation, is transparent to the host computers.

- **Master** – The physical router that is currently providing the virtual router interface to the host computers.

- **Owner** – The physical router that is configured with the IP address that is involved in the XRRP operation.

- **Advertisement Interval** – The time interval at which the Master router sends out XRRP packets on each virtual router interface.
Overview of XRRP Operation

XRRP allows you to configure pairs of HP 5300XL switches to behave as backup routers for each other. Each pair of routers configured to operate this way is defined as a Protection Domain. If either router in the Protection Domain fails for whatever reason, the other router will automatically take over the routing function of the failed router. This transfer of the routing function is transparent to the host computers that are using the routers.

To accomplish this transfer, both routers in the Protection Domain must have identical network access so that each can get to all the same subnets and the same end nodes without going through each other.

Figure 11-1 shows an example of a Protection Domain being used to provide redundant connectivity between some clients and the network servers that the hosts need to access. As part of the XRRP configuration, you define the identity of the Protection Domain. In figure 1, it is Domain 2. See “Configuring XRRP” on page 11-11 for information on how to configure XRRP.

Figure 11-1. XRRP Protection Domain

The clients are connected to the routers through a Layer 2 switch (in this case an HP Procurve Switch 4100GL).
Router Redundancy Using XRRP
Overview of XRRP Operation

XRRP During Normal Router Operation

For each router, XRRP defines a virtual router, using the IP address that you have configured on the router interface, and for which XRRP assigns a virtual MAC address based on the Protection Domain ID and the XRRP router number of the router that owns the interface. The configuration is done for each VLAN on which you wish to use XRRP for router redundancy, so the router interfaces for each virtual router must be in the VLAN. Each Protection Domain contains two routers, but within a single VLAN, up to 16 Protection Domains (16 pairs of routers) can be configured.

In the situation in which both routers in the Protection Domain are operating normally, none of the VLANs are down, each physical router behaves as the Master of all of its XRRP virtual router interfaces. The Master and Owner of each interface is the same.

In the example shown in figure 11-2, the XRRP configuration is done in VLAN 5. For Domain 2, Router-1 is given the IP address of 10.1.1.1 and Router-2 is given the address 10.1.1.2. XRRP assigns MAC addresses MAC-A to Router-1 and MAC-B to Router-2. Note that the clients in figure 2 use both of the virtual router as their default gateways. Client 10.1.1.48 is configured to use virtual router 10.1.1.1 as its default gateway, and client 10.1.1.49 is configured to use virtual router 10.1.1.2. In this way XRRP can be used to provide load balancing as long as both virtual routers are operating normally. The virtual routers will route packets passed to them, respond to IP ARP requests and PING packets, and perform the other router functions.

Figure 11-2. XRRP During Normal Router Operation
XRRP Fail-Over Operation

If all access to a VLAN from one of the routers in the Protection Domain fails, the routing function of that router is automatically transferred to the other router in the Protection Domain. The master of the virtual router in the Protection Domain sends out multicast advertisements at the XRRP advertisement interval (every 5 seconds by default). If the other router in the Protection Domain does not hear an advertisement packet within 3 advertisement intervals, this other router will become the master router, and it takes control of the IP address and the MAC address of the failed router.

Single VLAN Operation

In figure 11-3, the link between the layer-2 switch and Router-2 fails. As a result, Router-2 no longer hears any link signals on VLAN 5 and the communication between Router-2 and Router-1 is disabled. Router-1, after not hearing XRRP packets from Router-2, will take over the IP addresses from Router-2 for the VLAN 5 interfaces and it will take over the XRRP MAC address for Router-2. Now Router-1 is the Master for its own IP addresses and the IP addresses for Router-2 for VLAN 5, and it is the Master of its own XRRP MAC address and the XRRP MAC address for Router-2. As far as the clients are concerned, the transfer of router functionality is transparent – they can still get to the servers using the same IP addresses and MAC addresses as before.

Figure 11-3. XRRP Fail-Over Example
**Note**

Figure 11-3 shows a single interface on VLAN 5, but multiple interfaces could exist. For the fail-over to occur, Router-2 must have lost communication on all the VLAN 5 interfaces.

When the fail-over occurs, Router-1 would take over as the Master of the IP address for Router-2 on VLAN 5. If Router-2 has multiple IP addresses on VLAN 5, a multinet situation, Router-1 takes over all the IP addresses for Router-2 on VLAN 5.

**Multiple VLAN Operation**

If a router has XRRP interfaces in multiple VLANs, there are some additional details in the way that XRRP operates. For each VLAN on which you wish to run XRRP, a virtual router interface is created.

**Total Router Fail-Over.** In the multiple VLAN case, fail-over again occurs when XRRP packets are not heard on at least one of the VLANs from the other virtual router in the Protection Domain. Even if one or more VLANs are still operating correctly, when one VLAN fails (a link signal is no longer detected by the router from any device in the VLAN), the router with the failed VLAN will stop its operation as the Master of its owned virtual router interfaces. The fail over is a “total router” fail over. The router with the failed VLAN stops routing on all of its XRRP virtual interfaces and the other router in the Protection Domain takes control of all the XRRP IP and MAC addresses.

Depending on whether the routers can maintain communication through at least one or the XRRP VLANs (the VLAN continues to operate correctly for both routers in the Protection Domain), the type of fail-over varies:

- If communication is maintained, the router with the failed VLAN can execute what is called a “fast fail-over”. This situation is depicted in figure 11-4.

- If all XRRP communication is lost between the routers in the Protection Domain, the normal fail-over occurs after 3 advertisement intervals, as shown in figure 11-5.
**Fast Fail-Over.** As shown in figure 11-4, if the same link goes down as was shown in figure 11-3, the standard fail-over does not occur. As soon as Router-2 detects the loss of link signal from any device in VLAN 5, it immediately requests, through VLAN 6, that Router-1 to take over all of its virtual router resources. This function is referred to as “fast fail-over”. Because it occurs as soon as link signal is lost, the fail-over can take as little as one second to complete.

When Router-2 makes the fast fail-over request, if Router-1 has no failed VLANs, then it will take control of Router-2’s virtual interfaces. If Router-1 also has one or more failed VLANs, then it will not take control and both routers will continue to control only their owned IP addresses.
Standard Fail-Over. In the multiple-VLAN situation in which all communication between the routers in the Protection Domain is lost, the standard XRRP fail-over occurs. As shown in figure 6, Router-2 has lost communications on all of its XRRP virtual router interfaces. In this case, Router-1 will no longer hear XRRP packets coming from Router-2. If that condition persists for 3 advertisement intervals, Router-1 then takes over all of the virtual routers from Router-2.

Figure 11-5. Standard XRRP Fail-Over with Total VLAN Failure

If the cause of the total VLAN access failure, as shown in figure 17-5, is because of a complete router failure (due to building power loss, for example), the router that remains active will wait for the three XRRP advertisement intervals and will then take control of the failed router’s IP and MAC addresses. If both routers are still active but the all network connections between them have been severed, then both routers will take over for each other. This means that identical IP and MAC addresses will exist on both routers, but in a completely severed network, there will be no duplicated MAC or duplicate IP address errors.
If Communication is Maintained Through Non-XRRP Interfaces. In some cases, it may be possible that all connectivity is lost between the routers on all their XRRP virtual router interfaces, in which case XRRP operates and both routers try to take control of all the virtual routers in the Protection Domain, but if connectivity still exists on non-XRRP VLANs, a situation could occur in which both routers allow and use the same MAC addresses on the non-XRRP VLAN(s). This could create a situation in which a switch connected between the two routers will see continuous move interrupts and potential duplication of inbound packets if that switch floods. To prevent this condition, a simple XRRP protocol packet is exchanged between the two routers on the non-XRRP VLAN to inform each other of their uses of the MAC addresses. This exchange prevents the routers from taking over each other’s MAC addresses. Note that this protocol is used only when one router attempts to take over control of the other routers virtual router interfaces.

XRRP Operation Notes

- **Reserved Multicast MAC Address** – XRRP uses the following multicast MAC address for its protocol packets: *0101-E794-0640*

- **Use of Proxy ARP on non-XRRP VLANs** – Although it is not disallowed, you should not configure Proxy ARP on non-XRRP VLANs on a router running XRRP. To do so will potentially cause loss connectivity on those non-XRRP VLANs should the router fail-over to the other router in the Protection Domain.

The non-XRRP VLANs will not fail-over, however the XRRP-assigned MAC address, which were used while the router was operating as an XRRP router, were used on *all* the router interfaces, XRRP and non-XRRP. When the router fails-over its XRRP interfaces, it stops operating as an XRRP router and reverts back to using the default factory-assigned MAC address on all the interfaces. Any hosts that rely on proxy ARP will only receive updated ARPs for the router MAC address not for all the possible IP addresses that the router had previously responded too as a proxy ARP interface. Note: this is not a problem on the XRRP interfaces because the XRRP-assigned MAC address will have moved over to the other router and proxy ARP learned routes will still be valid. (See also “Router connectivity” on the next page).

- **Static and Default route usage** – You should never set up a default or static route that points to the peer XRRP router as the path. Should fail-over occur, this path is no longer valid and connectivity on that path will be lost.
Router Redundancy Using XRRP

Overview of XRRP Operation

- **Router connectivity** – In general peer routers using XRRP must have identical connectivity. That is, they must have the same access to all remote subnets, and the route costs of the access must be the same. This will prevent the routing protocols from using the peer XRRP router as the best path to get to a given subnet.

  If this is not done, then fail-over may have to wait until the routing protocols converge before full connectivity is restored. Should one router have exclusive access to a given subnet, (that is, the only way one of the XRRP routers can get to a given subnet is though its peer) connectivity to those exclusive subnets may be lost when fail-over occurs.

- **SNMP Requests** – SNMP requests on an XRRP router interface will follow the virtual interface, which may be different from the physical interface in a fail-over situation. Alternately, you can make sure that the SNMP requests are made on the management VLAN or other non-XRRP interface.

- **Multiple VLAN Considerations** – When using multiple VLANs, some consideration must be given to whether the router interfaces on the Series 5300XL are connected to devices that have a **multiple forwarding database** (a MAC address table for each VLAN):
  - If the switch at the other end of a router interface connection has a multiple forwarding database, you can use a separate interface for each VLAN. Since the switch at the other end has a separate MAC address table for each VLAN, the fact that the Series 5300XL Switches uses the same MAC address on all interfaces causes no problems.

![Diagram showing network topology with 4108GL and 5308L switches]

**Figure 11-6. Example of a Valid Topology for Devices Having Multiple Forwarding Databases in a Multiple VLAN Environment**

As of this printing, the HP Procurve switches that have a multiple forwarding database include the Series 5300XL switches, the Series 4100GL Switches, the Switch 2650, and the Switch 6108.
If the switch at the other end of the router interface connection does not have a multiple forwarding database, you can use only a single interface for the connection. For multiple VLANs, use VLAN tagging. To increase the network bandwidth of the connection between the router and the switch, use a trunk of multiple physical links rather than a single physical link.

As of this printing, the HP Procurve switches that do not have a multiple forwarding database include the Switches 1600M, 2400M, 2424M, Series 2500, 4000M, and 8000M. Some older HP AdvanceStack switches also do not have a multiple forwarding database.

For more information, refer to “Multiple VLAN Considerations” on page 2-17.

**Configuring XRRP**

Configuring XRRP is performed through the switch console CLI at the global configuration level by using the `xrrp` command. Use the `xrrp ?` command to see a list of possible options. You define which VLANs have XRRP configured through the `xrrp instance` command described on page 11-13.

You should first customize the XRRP configuration, as described below, and then enable XRRP, as described on page 11-15. Some of the configuration parameters cannot be changed while XRRP is operational. These are identified in the parameter descriptions below.
Customizing the XRRP Configuration

To customize the XRRP configuration, use any of the following XRRP command options at the CLI global configuration level:

**Syntax:**

```
xrrp domain < 1-16 >
no xrrp
```

```
xrrp [ router < 1-2 >]
```

```
xrrp failback < 10-999 >
```

```
xrrp trap < trap-name | all >
```

```
xrrp instance < owner-router-number > < vlan-id > [ advertise < 1-60 > | authentication < auth-string > | ip < ip-addr/mask-length > ]
```

**xrrp domain < 1-16 >**

This command sets the XRRP Protection Domain that the router is in. The router can be in only one domain. The default value is 1. This value cannot be changed if there is at least one virtual router instance running on the router. To change the value after XRRP is operating, you must first disable XRRP (use the **no xrrp** command).

**xrrp router < 1-2 >**

This command sets the unique number for the router within a given Protection Domain. No two routers in the same Protection Domain can have the same router number. The default value is 1.

This value cannot be changed if there is at least one virtual router instance running on the router. To change the value after XRRP is operating, you must first disable XRRP (use the **no xrrp** command).
**xrrp failback < 10-999 >**

This command sets the XRRP fail back time in seconds. The fail back time is the delay that a router will wait before trying to take back control of all the XRRP virtual routers it owns after its VLANs come back up. The default time is 10 seconds.

**[no] xrrp trap < trap-name | all >**

This command enables or disables the generation of SNMP traps for XRRP events on the router. The following trap names are available:

- **state-change** – signifies that the router has a experienced a state change. The trap sent would contain the **domain-number**, **router-number**, and state information.

- **master-transition** – signifies that the router state has changed specifically to the master state. The trap sent would contain the **domain-number**, **router-number**, and state information.

- **authentication-failure** – signifies that the virtual router instance has received an XRRP packet with an authentication mismatch. The trap sent would contain the **domain-number**, **router-number**, and virtual router instance ID (virtual router owner number and VLAN ID) of the virtual router that detected the error.

To enable all the traps, use the command **xrrp trap all**.

To disable the traps, use the **no** form of the command, with the trap name to disable a specific trap or with **all** to disable all the traps. By default, all the traps are disabled.

**[no] xrrp instance < owner-router-number > < vlan-id >**

This command configures the virtual router interface on the router. The virtual router interface (XRRP instance) is identified by the **owner-router-number** and the **vlan-id**. The **owner-router-number** is the XRRP router number of the router that owns the IP address(es). The **vlan-id** identifies the VLAN on which the XRRP instance is running.

**Required Parameters** – For each router in the Protection Domain, an **xrrp instance** command must be entered for each of the following:

- To create each virtual router interface for the physical router being configured, you would enter an **xrrp instance** command with the router number and the VLAN ID for that interface. For example, to create a virtual router interface in VLAN 5 for the router that has the XRRP router number 1, you would enter the following command:

  xrrp instance 1 5
• To specifically identify the virtual router interfaces on the other router in the Protection Domain, you would enter an `xrrp instance` command with the `ip` parameter. For example, on Router-1 in VLAN 5, to identify the virtual router interface on Router-2 that has the IP address 10.1.1.2 and mask length 24, you would enter the following command:

```
xrrp instance 2 5 ip 10.1.1.2/24
```

For the instance command that creates the virtual router interface on the router being configured, the `ip` parameter must not be specified. These XRRP instances, which are being configured on the router that owns the IP address, automatically use the IP address of the VLAN on the router being configured.

Please see the configuration examples on page 11-16 to help clarify these concepts.

• If a VLAN has multiple IP addresses (a multinet situation), an individual IP address can be removed from the XRRP configuration. To remove an IP address from fail-over protection by the router being configured, use the `no` version of the instance command. For example, to remove the virtual interface in the above example from the fail-over protection provided by Router-1, you would enter the following command:

```
o xrrp instance 2 5 ip 10.1.1.2/24
```

You cannot remove an individual IP address if it is the only IP address associated with the backup router.

**Variable Parameters** – In addition, the following variable parameters can be specified by the `xrrp instance` command:

- **advertise < 1-60 >** – this parameter specifies the frequency, in seconds, that the XRRP Master sends out XRRP advertisement packets. The default is 5 indicating that the Master sends out a packet every 5 seconds.

- **authentication < auth-string >** – this parameter sets the string that is used by the virtual router instance for the authentication of the received XRRP packets. The string can be up to 8 characters long. This same string must be configured on all the virtual routers in the Protection Domain that wish to use authentication.

  By default, there is no authentication. Use the `no` version of the command to disable the authentication that was previously enabled on the virtual router interface.

---

**Note**

For every VLAN on which you wish to run XRRP, you must first configure the VLAN with an IP address.
Enabling and Disabling XRRP

_Syntax:_  
\[no\] xrrp

Once you have completed the XRRP customization, as described in the previous section, use the `xrrp` command by itself to enable XRRP operation on the switch for all VLANs on which XRRP has been configured. Use the `no xrrp` command to disable all XRRP operation on the switch.

**Configuration Rules**

- XRRP can be configured only on statically configured IP VLANs. VLANs automatically created by GVRP cannot be used.
- XRRP cannot be configured on the management VLAN or on any VLAN that gets its IP address through DHCP or Bootp.
- XRRP must be disabled before the Protection Domain number or the router number configuration can be changed. Use the `no xrrp` command to disable XRRP.
- Dynamic reconfiguration – You should be aware that although XRRP can be reconfigured while it is running, dynamic configurations can lead to inconsistency between the two routers while the configuration changes are in progress. This will potentially result in error log messages until the configurations are consistent (for example, matched IP addresses for primary on one side and secondary on the other). To avoid these logs, disable XRRP while changing its configuration.

Use the `no xrrp` command to disable XRRP.
Configuration Examples

The following configuration examples create the XRRP setups in the single VLAN and multiple VLAN environments shown in the figures earlier in this chapter.

Configuration for Figure 11-2 – Single VLAN Example

See the figure on page 11-4.

<table>
<thead>
<tr>
<th>Router-1 Configuration</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPswitch (vlan-5)# ip address 10.1.1.1/24</td>
<td>Configures the IP address of the router interface in VLAN 5.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp domain 2</td>
<td>Sets the identity of the Protection Domain.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp router 1</td>
<td>Sets the XRRP router number.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 5</td>
<td>Creates the XRRP virtual router interface.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 5 ip 10.1.1.2/24</td>
<td>Identifies the virtual router interface on Router-2 for which Router-1 is providing fail-over protection.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp</td>
<td>Enables XRRP operation on Router-1.</td>
</tr>
<tr>
<td>HPswitch (config)# write memory</td>
<td>Saves this configuration to startup memory.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Router-2 Configuration</th>
<th>(the explanation is the same as for Router-1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPswitch (vlan-5)# ip address 10.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp domain 2</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp router 2</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 5</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 5 ip 10.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# write memory</td>
<td></td>
</tr>
</tbody>
</table>
Configuration for Figure 11-4 – Multiple VLANs

See the figure on page 11-7.

<table>
<thead>
<tr>
<th>Router-1 Configuration</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPswitch (vlan-5)# ip address 10.1.1.1/24</td>
<td>Configures the IP address of the router interface in VLAN 5.</td>
</tr>
<tr>
<td>HPswitch (vlan-6)# ip address 10.2.1.1/24</td>
<td>Configures the IP address of the router interface in VLAN 6.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp domain 2</td>
<td>Sets the identity of the Protection Domain.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp router 1</td>
<td>Sets the XRRP router number.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 5</td>
<td>Creates the XRRP virtual router interface in VLAN 5.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 5 ip 10.1.1.2/24</td>
<td>Identifies the virtual router interface on Router-2 for which Router-1 is providing fail-over protection in VLAN 5.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 6</td>
<td>Creates the XRRP virtual router interface in VLAN 6.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 6 ip 10.2.1.2/24</td>
<td>Identifies the virtual router interface on Router-2 for which Router-1 is providing fail-over protection in VLAN 6.</td>
</tr>
<tr>
<td>HPswitch (config)# xrrp</td>
<td>Enables XRRP operation on Router-1.</td>
</tr>
<tr>
<td>HPswitch (config)# write memory</td>
<td>Saves this configuration to startup memory.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Router-2 Configuration</th>
<th>(the explanation is the same as for Router-1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HPswitch (vlan-5)# ip address 10.1.1.2/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (vlan-6)# ip address 10.2.1.2/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp domain 2</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp router 2</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 5</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 5 ip 10.1.1.1/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 2 6</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp instance 1 6 ip 10.2.1.1/24</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# xrrp</td>
<td></td>
</tr>
<tr>
<td>HPswitch (config)# write memory</td>
<td></td>
</tr>
</tbody>
</table>
Displaying XRRP Data

To verify XRRP configuration and for XRRP status and statistics information display, use the following CLI show xrrp commands at either the Manager level or the global configuration level:

**Syntax:** show xrrp traps

This command displays the information on the configured XRRP traps.

```
HPswitch(config)# show xrrp traps
Status and Counters - XRRP Traps Information

| Trap Name             | Status |
|-----------------------+--------|
| state-change          | Enabled|
| master-transition     | Disabled|
| authentication-failure| Disabled|
```

**Syntax:** show xrrp config [global | instance [< owner-router-num > < vlan-id >]]

This command displays XRRP configuration information. Invoked without parameters it shows global and virtual routers configuration on the switch.

If the **global** keyword is specified, then the generic configuration information is displayed.

```
HPswitch(config)# show xrrp config global
Status and Counters - XRRP Global Configuration Information

  XRRP Enabled : Yes
  Domain Number : 2
  Router Number : 1
  Failback Delay : 11
```

The keyword **instance** can be used to display configuration information for the virtual router instance(s) on the switch. If no parameters are specified after this keyword, the information for all virtual routers is displayed, otherwise
the information for the particular virtual router is displayed by specifying the `owner-router-number` and the `vlan-id` in the command. In the example below, the configuration information for the virtual router number 1 on VLAN 5 is requested.

```
HPswitch(config)# show xrrp config instance 1 5

Status and Counters - XRRP Virtual Router Configuration Information

Owner Router Number : 1
VLAN ID : 5
Authentication Type : Simple Text Password
Authentication Key : password
Advertise Interval : 5

IP Address Subnet Mask
--------------- ---------------
10.1.1.1 255.255.248.0
10.2.1.1 255.255.248.0
```

**Syntax:** `show xrrp statistics [global | insta(<owner-router-num> <vlan-id>)] | router<router-num>]

This command displays XRRP status and statistics information.

If the keyword `global` is used, then generic information is displayed as shown in the next example.

```
HPswitch(config)# show xrrp statistics global

Status and Counters - XRRP Global Statistics Information

XRRP Enabled : Yes
This Domain Number : 2
This Router Number : 1
XRRP MAC Addr : 0001e7-940601
XRRP AND Mask : ffffff-ffffff
XRRP Up Time : 46 hours

Pkts Rx Corrupt Pkts Bad Version Bad Chksum Not Domain
--------------- --------------- --------------- --------------- ---------------
7 0 0 0 0
```
The keyword **instance** can be used to display statistics information for the virtual router instance(s) on the switch. If no parameters are specified after this keyword, the information for all virtual routers is displayed, otherwise the information for the particular virtual router is displayed by specifying the **owner-router-number** and the **vlan-id** in the command. In the example below, the statistics information for the virtual router number 1 on VLAN 5 is requested.

```
HPswitch(config)# show xrrp statistics instance 1 5
```

**Status and Counters - XRRP Virtual Router Statistics Information**

- **Owner Router Number**: 1
- **VLAN ID**: 5
- **Operational State**: Master
- **Up Time**: 64 mins

<table>
<thead>
<tr>
<th>Pkts Rx</th>
<th>Pkts Tx</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>780</td>
</tr>
</tbody>
</table>

**Zero Priority Rx**: 0  
**Zero Priority Tx**: 0  
**Bad Version Pkts**: 0  
**Mismatched Pswd Pkts**: 0  
**Mismatched IP Pkts**: 0  
**Mismatched Interval Pkts**: 0

The keyword **router** can be used to display statistics information for the specific router coordinator operating in the XRRP domain as shown in the next example.

```
HPswitch(config)# show xrrp statistics router 2
```

**Status and Counters - XRRP Router Coordinator Statistics Information**

- **Router Number**: 2
- **Become Master**: 1
- **Master Time**: 76 mins

```
<table>
<thead>
<tr>
<th>Type1 Pkts Rx</th>
<th>Type1 Pkts Tx</th>
<th>Type2 Pkts Rx</th>
<th>Type2 Pkts Tx</th>
<th>Unknown VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>924</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
Comparison Between XRRP and VRRP

The following information compares the characteristics of XRRP and the industry standard VRRP.

- XRRP will allow a router to respond to SNMP requests on the virtual router IP address even if it is not the owner. VRRP does not. This would allow you to still access the failed router on VLANs that are accessible on that router.

- XRRP uses the same MAC address for each virtual router owned by a given physical router. VRRP uses a separate MAC address per virtual router.

- XRRP uses a fail-over domain concept with up to 2 routers in the fail-over domain and up to 16 domains connected to a given VLAN. VRRP uses a flat space with up to 255 virtual routers in a level 2 switch fabric. However these 255 virtual routers can be used over on every VLAN with VRRP.

- XRRP will warn you of mismatched configurations between the routers but will attempt to use the current master configuration whenever possible when these mismatches occur.

- VRRP fails over at the virtual router level allowing a given physical router to continue to route packets on those virtual routers that it still owns. XRRP will fail-over at the router level. If one of the virtual routers controlled by a physical router fails, then all the virtual routers that it owns will be taken over by the other router in the same XRRP Protection Domain.

- XRRP has fast fail-over. VRRP does not.
— This page is intentionally unused. —
Index

Numerics

802.1p priority (QoS)
  definition ... 8-5
802.1q VLAN in mesh ... 7-22
802.1Q VLAN standard ... 6-5
  use with QoS, definition ... 8-5
802.1w as a region ... 6-52
802.1x, mesh, not supported ... 7-5

deny any, implicit ... 9-10, 9-12, 9-13, 9-16, 9-17, 9-18, 9-26, 9-30, 9-31
deny any, implicit, supersede ... 9-27
deny any, implicit, switched packets ... 9-14
deny, defined ... 9-6
editing ... 9-32
effect of replacing ... 9-31
end ... 9-30
exit statement ... 9-30
extended, defined ... 9-6, 9-26
extended, numeric I.D. range ... 9-26
extended, structure ... 9-28
extended, use ... 9-8
filtering criteria ... 9-8
filtering process ... 9-13, 9-14, 9-18
host option ... 9-23
i.d. range, 1-99 ... 9-33
implicit deny
  See deny any, implicit.
implicit deny, defined ... 9-6
inbound traffic, defined ... 9-6
inverse mask
  See wildcard.
ip routing required ... 9-3, 9-4
IP routing requirement ... 9-11
ip routing requirement, exception ... 9-11
list entry sequence
  See sequence, ACEs.
logging ... 9-10
logging described ... 9-59
logging, ACLs ... 9-35
logging, performance impact ... 9-10
logging, session ... 9-10
mask ... 9-10, 9-21
mask, CIDR ... 9-32
mask, defined ... 9-6
mask, multiple IP addresses ... 9-24
mask, one IP address ... 9-23
match, always ... 9-31
match, criteria ... 9-22
match, example ... 9-23
match, ignored ... 9-18
maximum allowed ... 9-18, 9-33
name or number assignment ... 9-31
name string, maximum characters ... 9-26, 9-33

A

ABC
  in mesh domain ... 7-25

ABR
  definition ... 10-35
  OSPF ... 10-35

ACL
  ACE sequence ... 9-32
    See ACL, sequence, ACEs.
  ACE, defined ... 9-5
  ACE, duplicates ... 9-32
  ACE, limit ... 9-18
  ACE, order in list
    See sequence, ACEs.
  ACE, after match not used ... 9-29
  ACL ID, defined ... 9-5
  ACL log message
    See ACL, logging.
  ACL, defined ... 9-5
  applied to open connection ... 9-63
  assign nonexistent i.d. ... 9-31
  assign to VLAN ... 9-31
  basic structure ... 9-26
  broadcasts, effect on ... 9-63
  CIDR, mask ... 9-32, 9-34
  command summary ... 9-4
  command syntax ... 9-34
  configuration planning ... 9-10
  configured but not used ... 9-31
  configured, not used ... 9-31
  configuring offline ... 9-10
  copy operation appends ... 9-56
  create, CLI method ... 9-32
  DA, defined ... 9-6, 9-7
  definitions ... 9-5

Index – 1
nonexistent i.d., assign ... 9-31
number of entries ... 9-9
offline creation ... 9-56
operation with PIM ... 5-35
operator, comparison ... 9-40
outbound traffic, defined ... 9-7
performance degraded ... 9-10
permit, defined ... 9-7
planning ... 9-10, 9-16
policies ... 9-16
policy application points ... 9-3
ports affected ... 9-19
purpose ... 9-3
replacing ... 9-19
replacing active ACEs ... 9-31
routed traffic ... 9-19
routing requirement ... 9-18
rules, configuration ... 9-18
rules, operation ... 9-18
SA, defined ... 9-7
security use ... 9-3, 9-17
security use, caution ... 9-17
sequence, ACEs ... 9-32
source routing, caution ... 9-11, 9-25
standard, defined ... 9-7, 9-26
standard, example ... 9-35
standard, structure ... 9-27
standard, use ... 9-8, 9-33
static VLAN requirement ... 9-11, 9-19
supernetting ... 9-21
supersede implicit deny any ... 9-30
switched packets ... 9-14, 9-19
syntax
  See command syntax.
Syslog
  See ACL, logging.
TCP or UDP port number, IANA ... 9-41
terms ... 9-5
traffic types filtered ... 9-3, 9-10
types, defined ... 9-26
VLAN assignment ... 9-12
VLANs ... 9-19
where applied to traffic ... 9-12, 9-19
wildcard ... 9-6, 9-22, 9-23
wildcard, defined ... 9-7
ACL, standard numeric I.D. range ... 9-26
active path ... 6-3

address
  IP ... 10-10
administrative distance, OSPF ... 10-50
advertisement interval, XRRP
  configuring ... 11-14
definition ... 11-2
advertisement, GVRP
  definition ... 3-3
advertisement, OSPF ... 10-34
  area ... 10-40
  retransmit interval ... 10-45, 10-48
area range, OSPF
  configuring ... 10-42
area, OSPF
  assigning VLAN to ... 10-43
  configuring ... 10-40
  definition ... 10-34
  displaying area information ... 10-55
ARP
  cache ... 10-5
  cache table ... 10-5
  configuring parameters ... 10-11
  how it works ... 10-11
  proxy ... 10-13
ASBR
  definition ... 10-35
  OSPF ... 10-35
assigning
  IP address ... 10-10
authentication
  OSPF
    description ... 10-44
    MD5 ... 10-44, 10-48
    simple password ... 10-44, 10-48
authentication, XRRP
  configuring ... 11-14
auto port setting ... 4-5
automatic broadcast control
  See ABC.
Autonomous system, OSPF ... 10-34

B

bandwidth
  effect of QoS ... 8-1
bandwidth loss, spanning tree ... 6-49
blocked link from STP operation ... 6-8, 6-50
blocked port
from IGMP operation ... 4-5
from STP operation ... 6-7, 6-48
Bootp
gateway ignored ... 2-44
BPDU ... 3-3, 6-5
bridge protocol data unit ... 3-3
broadcast domain ... 2-3
broadcast storm ... 6-3, 6-9, 7-4
broadcast traffic ... 7-18
effect of ACL ... 9-63
enabling forwarding of directed ... 10-14

C

Caches
ARP ... 10-5
IP forwarding ... 10-6
CDP
mesh requirement ... 7-6
CIDR ... 10-10
CLI
configuring RSTP ... 6-12
configuring XRRP ... 11-12
configuration ... 6-7, 6-48, 10-19
ARP parameters ... 10-11
Class of Service ... 8-11
default route ... 10-19
DHCP Relay ... 10-73
factory default ... 2-21, 2-27, 6-7, 6-47
ICMP ... 10-15
IP routing forwarding parameters ... 10-13
IP routing parameters ... 10-10
IRDP ... 10-70
OSPF ... 10-34
RIP ... 10-21, 10-23
changing RIP type ... 10-24
enabling RIP ... 10-23
enabling route redistribution ... 10-26
redistribution ... 10-25
redistribution metrics ... 10-25
redistribution metric ... 10-26
router loop prevention ... 10-27
router ID ... 10-10
RSTP
from the CLI ... 6-12
from the menu ... 6-18
per-port parameters ... 6-16

whole switch parameters ... 6-14
spanning tree protocol ... 6-7, 6-48
static IP routes ... 10-17, 10-19
XRRP ... 11-11
configuration rules ... 11-15
examples ... 11-16
configuring RSTP ... 6-11
console, for configuring
switch meshing ... 7-10

CoS
See Class of Service.

D

DA, defined ... 9-6, 9-7
dedicated management VLAN ... 2-43
default route ... 10-19
affect of XRRP ... 11-9
DHCP
gateway ignored ... 2-44
DHCP Relay
configuration ... 10-73
enabling ... 10-74
helper address ... 10-74
minimum requirements ... 10-74
directed broadcasts ... 10-14
disabling
XRRP ... 11-15
displaying information
IRDP ... 10-72
domain ... 2-21, 2-27
domains, connecting ... 7-25
downstream device (QoS)
definition ... 8-5
effect of priority settings ... 8-7

DR (designated priority router)
OSPF ... 10-35
election ... 10-35
DSCP
Policy Table ... 8-51
policy, defined ... 8-5
See also priority.

E

enabling XRRP ... 11-15
enabling OSPF ... 10-40
enabling RIP ... 10-23
enabling RSTP
  CLI … 6-13
  menu interface … 6-18
  web browser interface … 6-20
enabling STP
  CLI … 6-13
event log
  See log.
examples
  XRRP configuration … 11-16
Exclude Source
  See IGMP.
external LSA
  displaying … 10-56

F
fail-over
  XRRP … 11-5
fast fail-over, XRRP … 11-7
fast mode
  spanning tree … 6-22, 6-28
filters
  effect of IGMP … 4-21
  maximum allowed … 4-21
  OSPF redistribution
    configuring … 10-48
    displaying … 10-64
  RIP redistribution
    configuring … 10-25
    displaying … 10-33
forbid option
  See GVRP.
forwarding
  directed broadcasts … 10-14
forwarding database
  See VLAN.
forwarding parameters, IP routing
  configuring … 10-13
forwarding port, IGMP … 4-5

G
GARP
  See GVRP.
gateway, manual config … 2-44
global parameters
  OSPF … 10-39
RIP … 10-22
GVRP … 6-46
  advertisement … 3-19
  advertisement, defined … 3-3
  advertisement, responses to … 3-6
  advertisements, generating … 3-11
  auto option … 3-10
  benefit … 3-3
  block … 3-8
  CLI, configuring … 3-14
  configurable port options … 3-6
  configuring learn, block, disable … 3-8
  convert dynamic to static … 3-7
  converting to static VLAN … 3-3
  disable … 3-8
  dynamic VLAN and reboots … 3-19
  dynamic VLANs always tagged … 3-4
  forbid option … 3-10
  GARP … 3-3
  general operation … 3-4
  IP addressing … 3-7
  learn … 3-8
  learn, block, disable … 3-10
  menu, configuring … 3-13
  meshed ports … 7-23
  meshing requirement … 7-6
  non-GVRP aware … 3-18
  non-GVRP device … 3-18
  operating notes … 3-18
  port control options … 3-11
  port-leave from dynamic … 3-11
  reboot, switch … 3-11
  recommended tagging … 3-11
  standard … 3-3
  tagged, dynamic VLAN … 3-4
  unknown VLAN … 3-11
  unknown VLAN, options … 3-7
  VLAN behavior … 2-11
  VLAN, dynamic adds … 2-25
  VLAN, maximum … 3-18
  with QoS … 8-38

H - I
helper address for DHCP Relay … 10-74
hop count, mesh switch
  See mesh.
IANA … 9-41
ICMP
configuring ... 10-15
disabling messages ... 10-15
IEEE 802.1 standard ... 7-22
IGMP
benefits ... 4-3
configuration ... 4-11
configure per VLAN ... 4-5
effect on filters ... 4-21
Exclude Source ... 4-12
high-priority disabled with PIM ... 5-35
high-priority forwarding ... 4-5
in switch mesh domain ... 7-22
Include Source ... 4-12
IP multicast address range ... 4-21
leave group ... 4-12
maximum address count ... 4-21
mesh requirement ... 7-6
multicast group ... 4-11
multimedia ... 4-3
operation ... 4-11, 4-12
port states ... 4-5
query ... 4-11
report ... 4-12
status ... 4-12
traffic ... 4-5
Version 3 ... 4-12
inbound port (QoS)
definition ... 8-5
Include Source
See IGMP.
interface
changing cost of RIP routes ... 10-24
changing RIP type ... 10-24
OSPF
defaults ... 10-43
displaying information ... 10-57, 10-58
VLAN
enabling IRDP ... 10-71
XRRP configuration ... 11-13
interface parameters
OSPF ... 10-39
RIP ... 10-22
IP
gateway ... 2-44
traffic priority based on ToS field ... 8-24
IP address
assigning ... 10-10
CIDR notation ... 10-10
IP forwarding cache ... 10-6
IP global parameters ... 10-7
IP interface parameters ... 10-9
IP route exchange protocols ... 10-7
IP route table ... 10-5
IP routing
ARP cache table ... 10-5
changing ARP parameters ... 10-11
changing router ID ... 10-10
configuring static routes ... 10-17
default route ... 10-19
DHCP Relay configuration ... 10-73
directed broadcasts ... 10-14
forwarding cache ... 10-6
forwarding parameters ... 10-13
global parameters ... 10-7
ICMP
configuration ... 10-15
disabling messages ... 10-15
interface parameters ... 10-9
IRDP configuration ... 10-70
null static route ... 10-19
OSPF
area configuration ... 10-40
area information ... 10-55
assigning area range ... 10-42
configuration ... 10-34
displaying configuration and status ... 10-53
displaying routing table ... 10-68
enabling ... 10-40
enabling redistribution ... 10-50
general information ... 10-53
overview ... 10-34
redistribution information ... 10-64
overview ... 10-3
parameter configuring ... 10-10
Proxy ARP, enabling ... 10-13
required for ACLs ... 9-3, 9-4
RIP
configuration ... 10-21
displaying configuration and status ... 10-27
enabling ... 10-23
general information ... 10-28
interface information ... 10-30
overview ... 10-21
parameters and defaults ... 10-22
peer information ... 10-31
redistribution … 10-25
redistribution information … 10-33
restrict filter information … 10-33
route exchange protocols … 10-7
routing table … 10-5
static route configuration … 10-19
static route types … 10-17
tables and caches … 10-4
VLAN interface … 10-4
IP, type of service
  configuring priority … 8-24
IRDP
  configuring … 10-70
  displaying information … 10-72
  enabling globally … 10-71
  enabling on VLAN interface … 10-71
L
LACP
  mesh, effect … 7-5
latency
  reducing with switch meshing … 7-19
latency, decrease … 7-19
leave group
  See IGMP.
legacy VLAN … 2-10
link failure … 7-2
links, redundant, in mesh … 7-25
load-balancing … 7-2
log, counter … 5-37
log, PIM messages
loop, network … 6-5, 6-7, 6-48
LSA
  displaying … 10-60
  external
    displaying … 10-56
    reduction … 10-36
M
MAC address
  duplicate … 2-17
  same for all VLANs … 2-52
  single forwarding database … 2-17
MAC address table, per switch … 11-10
MAC address table, per VLAN … 11-10
MAC address, multiple … 11-10
MAC address, per switch … 2-17
MAC address, per VLAN … 2-17
master, XRRP
  definition … 11-2
maximum VLANs, GVRP … 3-18
MD5 authentication
  OSPF … 10-44, 10-48
menu interface
  configuring RSTP … 6-18
mesh
  802.1x not supported … 7-5
  ABC … 7-9, 7-25
  backward compatibility … 7-7
  benefits … 7-2
  blocked ports … 7-10
  broadcast storm … 7-4
  broadcast traffic … 7-18
  broadcast tree … 7-19
  CDP … 7-6
  configuring from the console … 7-10
  connecting domains … 7-25
  connecting multiple domains … 7-6
  domain … 7-3
  domain, bringing up … 7-9
  domain, defined … 7-4
  dynamic vlan … 7-23
  edge switch … 7-4, 7-18
  filtering … 7-22
  GVRP … 7-23
  GVRP requirement … 7-6
  hop count … 7-5, 7-24
  See mesh, hop count.
  hub not allowed … 7-5, 7-7
  IGMP requirement … 7-6
  increase STP cost … 7-21
  IP routing not allowed … 7-5
  LACP dynamic trunk, effect … 7-5
  link blocked … 7-21
  link to non-mesh switch … 7-20
  links, multiple … 7-25
  management VLAN … 2-48
  maximum domain size … 7-24
  multicast traffic … 7-18
  multiple mesh domains … 7-21
  multiple VLANs … 7-19
  no Type selection … 7-25
  operating details … 7-18
  operating notes … 7-18
operating rules … 7-5
port limit per-switch … 7-5
port trunk … 7-25
port types … 7-2
redundant link … 7-21
redundant links … 7-4, 7-24, 7-25
redundant paths … 7-3
removing a port, effect … 7-5
RSTP … 7-5, 7-20
RSTP caution … 7-22
RSTP edge-port mode … 7-21
spanning tree … 6-53, 7-20
spanning-tree requirement … 7-5
static VLANs … 7-22
status, viewing … 7-14
STP … 7-5, 7-20
STP caution … 7-22
switch hop count … 7-25
switch limit per-domain … 7-5
trunked links not allowed … 7-5, 7-7
Type setting … 7-12
unicast … 7-19
utilization … 7-18
VLAN … 7-22
VLAN, dynamic … 7-6
VLAN, static … 7-6
with IGMP … 7-22
with network monitor port … 7-25
message
VLAN already exists … 2-37
metric
OSPF
    redistribution … 10-49, 10-50
RIP
    changing interface value … 10-24
    redistribution … 10-26
Modifying
OSPF compliance setting … 10-52
OSPF default port parameters … 10-52
MSTI, configuration … 6-63
MSTP
    See spanning-tree, 802.1s.
multicast group
    See IGMP.
multicast traffic … 7-18
multimedia
    See IGMP.
multiple … 2-17
multiple forwarding database … 2-17, 11-10
multiple-forwarding database … 2-17

N - O
NAT
    See routing.
neighbor
    OSPF … 10-45
        displaying information … 10-62
network address translation
    See routing.
null static route … 10-19
operating notes
    switch meshing … 7-18
optimizing RSTP configuration … 6-11
OSPF
    administrative distance … 10-50
    area … 10-34
    assigning VLAN to … 10-43
    configuring … 10-40
    area range
        configuring … 10-42
    ASBR … 10-35
    authentication
        description … 10-44
        MD5 … 10-44, 10-48
        simple password … 10-44, 10-48
    autonomous system … 10-34
    configuration rules … 10-39
    configuring … 10-34
    displaying information … 10-53
    area … 10-55
    external LSA … 10-56
    interface … 10-57, 10-58
    LSA … 10-60
    neighbor … 10-62
    redistribution … 10-64
    route … 10-68
    virtual link … 10-66
    virtual neighbor … 10-65
    DR (designated router) … 10-35
    election … 10-35
    enabling … 10-40
    global parameters … 10-39
    interface
        defaults … 10-43
        displaying information … 10-57, 10-58
interface parameters ... 10-39, 10-44
LSA
displaying information ... 10-56
modifying port parameters ... 10-52
neighbor ... 10-45
overview ... 10-34
parameters ... 10-39
redistribution
displaying ... 10-64
enabling ... 10-50
metric ... 10-49
metric type ... 10-50
redistribution filters
configuring ... 10-48
displaying ... 10-64
RFC compliance ... 10-36, 10-52
stub area ... 10-41
transit area ... 10-45
trap ... 10-51
virtual link ... 10-45
displaying information ... 10-66
parameters ... 10-47
virtual neighbor
displaying information ... 10-65
outbound port (QoS)
definition ... 8-5
outbound port queue (QoS)
definition ... 8-5
overview, IP routing ... 10-3
owner, XRRP
definition ... 11-2

P
parameters
IP global ... 10-7
IP interface ... 10-9
OSPF ... 10-39
interface ... 10-44
virtual link ... 10-47
path cost ... 6-7
peers, RIP
displaying information ... 10-31
Perlman, Interconnections ... 6-30
PIM error message ... 5-37
PIM-DM
age-out, multicast group entry ... 5-25
bandwidth conservation ... 5-8
bandwidth use ... 5-3
common subnet requirement ... 5-6
compatible draft versions ... 5-4
correlation ... 5-11, 5-12, 5-13, 5-14, 5-21, 5-29
correlation order ... 5-12
correlation, general elements ... 5-9
correlation, router ... 5-12
default settings recommended ... 5-9
displaying data and configuration ... 5-22
draft version 3 ... 5-3
draft versions 1 and 2 ... 5-4
error message ... 5-37
expiry time ... 5-26, 5-33
extended branch ... 5-5
features ... 5-4
flood ... 5-6
flood and prune ... 5-3, 5-6, 5-7, 5-27
flood and prune cycle ... 5-34
flood and prune technique ... 5-3
flow ... 5-6, 5-9
flow, bridged ... 5-36
flow, equalizing ... 5-35, 5-37, 5-38, 5-39, 5-40
flow, hardware ... 5-10, 5-13
flow, multicast, limit ... 5-10, 5-37
flow, software ... 5-10, 5-13
flow, VLAN limit ... 5-4
forwarding state ... 5-7
general application ... 5-3
general operation ... 5-4
graft packets ... 5-16, 5-17
group entry, age-out ... 5-25
hello hold-time ... 5-15, 5-29
hello interval, effect ... 5-15
host ... 5-9
IGMP required, per VLAN ... 5-9
IGMP requirement ... 5-3, 5-35
IGMP version 1 ... 5-4
IGMP version 2 ... 5-4
IGMP version 3 ... 5-4
IGMP, per VLAN ... 5-5
IP address required ... 5-35, 5-38
join ... 5-5, 5-6, 5-9
limit, multicast flow ... 5-10
log message ... 5-36, 5-37
log message counter operation ... 5-37
MIB support ... 5-4
MRT ... 5-4, 5-10, 5-13, 5-30, 5-36
MRT, explained ... 5-9
multicast address … 5-4, 5-10
multicast flow, limit … 5-10
multicast group address
  See multicast address.
multicast router, multiple … 5-31
Multicast Routing MIB … 5-4
multicast routing table
  See MRT … 5-4
multicast routing, defined … 5-10
multicast server … 5-10, 5-23, 5-33
OSPF … 5-5
outbound VLAN limit … 5-10
PIM instance per VLAN … 5-10
prune … 5-6, 5-10, 5-26, 5-32
prune delay … 5-17, 5-18
prune state … 5-7
pruned branch … 5-5
prune-pending state … 5-18
pruning … 5-3, 5-7
reverse path forwarding … 5-5
RFC 2932 … 5-4
RFC 2932 exceptions … 5-41
RFCs, applicable … 5-40
RIP … 5-5
route data … 5-23
router configuration … 5-12
routing protocol … 5-5, 5-9
routing switch 9300 … 5-34
RPF … 5-5
S/G pair … 5-9, 5-10
SNMP traps … 5-13, 5-27
source address, unicast … 5-10
state refresh … 5-7, 5-8, 5-13, 5-25, 5-27, 5-30, 5-33, 5-34
state refresh, on other routers … 5-34
static route … 5-5
subnet, common … 5-6, 5-10
time-to-live threshold … 5-19, 5-24
traps, SNMP … 5-13, 5-27
tree, multicast … 5-5, 5-6
TTL zero … 5-37
unicast routing … 5-3, 5-4, 5-5
unicast source address … 5-4
unicast source address, server … 5-10
version differences … 5-39
VLAN support, inbound … 5-4
VLAN support, outbound … 5-4
VLAN, flow limit … 5-4
VLAN, multinetted … 5-6
VLAN, PIM instance per … 5-10
XRRP … 5-4
port
  auto, IGMP … 4-5
  blocked by STP operation … 6-7, 6-48
  blocked in mesh … 7-10
  blocked, IGMP … 4-5
  forwarding, IGMP … 4-5
  loop … 6-7, 6-48
  monitoring … 2-52
  redundant path … 6-7, 6-48
  state, IGMP control … 4-5
port trunk
  meshed switch … 7-25
  VLAN … 2-52
  with fast-uplink STP … 6-42
port-based access control, no mesh … 7-5
precedence bits (QoS)
  definition … 8-5
primary VLAN
  See VLAN.
priority … 4-5
  802.1p priority, defined … 8-5
  802.1Q tagged VLAN … 8-5
codepoint, defined … 8-5
downstream device, defined … 8-5
dSCP policy, defined … 8-5
dSCP, defined … 8-5
inbound port, defined … 8-5
outbound port, defined … 8-5
upstream device, defined … 8-5
priority (QoS)
  criteria for prioritizing packets … 8-8
  protocol priority … 8-36
type of service screen … 8-24
VID, effect of eliminating … 8-38
VLAN ID priority … 8-38, 8-43
priority QoS)
  device priority screen … 8-19
  IP address, source and destination match … 8-19
Protection Domain, XRRP
  definition … 11-2
protocol priority (QoS)
configuring ... 8-36
protocols
   IP route exchange ... 10-7
proxy ARP
   effect of XRRP ... 11-9
   Proxy ARP, enabling ... 10-13

Q
Quality of Service
   basic operation ... 8-6
   configuring ... 8-11, 8-13
   configuring in browser interface ... 8-56
   configuring IP type of service ... 8-24
   criteria for prioritizing outbound packets ... 8-8
   definitions of terms ... 8-5
   device priority screen ... 8-19
   DSCP Policy Table ... 8-51
   GVRP not supported ... 8-38
   maximum entry limit ... 8-7, 8-58
   no override definition ... 8-10
   No override, effect of ... 8-52
   overview ... 8-1
   prioritizing traffic based on IP ToS field ... 8-24
   priority settings map to outbound queues ... 8-7
   priority settings mapped to downstream
   devices ... 8-7
   protocol priority screen ... 8-36
   type of service screen ... 8-24
   VLAN ID priority ... 8-38, 8-43
query
   See IGMP.
quick start ... 1-7

R
Rapid Spanning-Tree
   See RSTP
reboot ... 3-11
redistribution
   global RIP parameters ... 10-22
   into RIP ... 10-25
   metric
      OSPF ... 10-49
      RIP ... 10-26
   RIP
      displaying ... 10-33
      enabling ... 10-26
redistribution filters
   OSPF
      configuring ... 10-48
      displaying ... 10-64
   RIP
      configuring ... 10-25
      displaying ... 10-33
      redundant link ... 7-21
      redundant link, non-meshed ... 7-20
      redundant links ... 7-4
      redundant path ... 6-7, 6-48
      spanning tree ... 6-7
      region ... 6-47
      See spanning-tree, 802.1s.
report
   See IGMP.
restrict redistribution
   OSPF
      configuring ... 10-48
      displaying ... 10-64
   RIP
      displaying ... 10-33
revision number ... 6-51
RFC 2178 ... 10-36
RFC 2178 compliance
   enabling for OSPF ... 10-52
RFC 2932 ... 5-4
RFC 2932 MIB exceptions ... 5-41
RFCs, PIM-applicable ... 5-40
RIP
   changing RIP type ... 10-24
   changing route loop prevention ... 10-27
   changing the RIP metric ... 10-24
   configuring ... 10-21, 10-23
   displaying information ... 10-27, 10-28
   displaying interface information ... 10-30
   displaying peer information ... 10-31
   displaying redistribution information ... 10-33
   displaying restrict information ... 10-33
   enabling ... 10-23
   global parameters ... 10-22
   OSPF
      displaying ... 10-64
      enabling ... 10-50
      metric type ... 10-50
   RIP
      displaying ... 10-33
      enabling ... 10-26
interface parameters ... 10-22
overview ... 10-21
parameters and defaults ... 10-22
redistribution ... 10-25
displaying ... 10-33
enabling ... 10-26
metric ... 10-26
redistribution filters
configuring ... 10-25
displaying ... 10-33
route loop prevention, RIP configuration ... 10-27
route table
OSPF
displaying ... 10-68
router ID
changing ... 10-10
router, multicast, with IGMP ... 4-11
routing
configuring static routes ... 10-17
default route ... 10-19
DHCP Relay configuration ... 10-73
IP static routes ... 10-18, 10-19
IRDP configuration ... 10-70
NAT ... 10-76
client limit ... 10-77
configuration ... 10-77
displaying configuration ... 10-79
displaying status ... 10-79
example ... 10-78
general operation ... 10-76
hidden region ... 10-76
intended application ... 10-79
IP address mapping ... 10-77
operating notes ... 10-79
operating rules ... 10-77
private region ... 10-76
public region ... 10-76
requires routing enabled ... 10-77
TCP/UDP ... 10-79
null static route ... 10-19
OSPF
area configuration ... 10-40
area information ... 10-55
assigning area range ... 10-42
displaying configuration and status ... 10-53
displaying routing table ... 10-68
enabling ... 10-40
enabling redistribution ... 10-50
general information ... 10-53
overview ... 10-34
redistribution information ... 10-64
OSPF configuration ... 10-34
RIP
collection ... 10-21
displaying configuration and status ... 10-27
enabling ... 10-23
general information ... 10-28
interface information ... 10-30
overview ... 10-21
parameters and defaults ... 10-22
peer information ... 10-31
redistribution ... 10-25
redistribution information ... 10-33
restrict filter information ... 10-33
source-routing, caution ... 9-11, 9-25
static route types ... 10-17
RSTP
configuring ... 6-11
configuring per-port parameters ... 6-16
configuring whole switch parameters ... 6-14
configuring with the CLI ... 6-12
configuring with the menu ... 6-18
edge-port parameter ... 6-18
enabling from CLI ... 6-13
enabling from the menu ... 6-18
enabling with the web browser ... 6-20
mcheck parameter ... 6-16
meshing ... 7-20
meshing requirement ... 7-5
optimizing the configuration ... 6-11
path-cost parameter ... 6-16
point-to-point-mac parameter ... 6-16
priority parameter ... 6-16
viewing the configuration ... 6-12
RSTP, edge-port mode, meshing ... 7-21
S
SA ... 9-7
security, ACL
See ACL, security use.
server
access failure ... 6-6
setup screen ... 1-7
show commands
XRRP ... 11-18
single forwarding database ... 2-17
single point of failure ... 7-2
source-routing, caution ... 9-11, 9-25
spanning tree
  802.1Q standard ... 6-5
  802.1s
    See spanning tree, 802.1s.
  blocked link ... 6-8, 6-50
  blocked port ... 6-7, 6-48
  BPDU ... 6-5
  broadcast storm ... 6-3, 6-9
  caution, fast-uplink ... 6-30
  configuring per-port parameters ... 6-16
  configuring RSTP ... 6-11
  configuring whole-switch parameters ... 6-14
  configuring with the menu ... 6-18
  description of operation ... 6-7
  enabling from the browser interface ... 6-43
  enabling in the CLI ... 6-26
  enabling MSTP ... 6-69
  enabling RSTP ... 6-13
  enabling STP ... 6-13
  fast mode ... 6-22, 6-28
  fast-uplink terminology ... 6-31
  fast-uplink, configuring ... 6-41
  fast-uplink, menu ... 6-33
  fast-uplink, operating notes ... 6-42
  fast-uplink, viewing status, CLI ... 6-39
  fast-uplink, viewing status, menu ... 6-37
  fast-uplink, with port trunks ... 6-42
  loop, network ... 6-5
MSTP
  See spanning-tree, 802.1s
  operation with switch meshing ... 7-20
  redundant path ... 6-3
  RSTP edge port parameter ... 6-16
  RSTP mcheck parameter ... 6-16
  RSTP path-cost parameter ... 6-16
  RSTP point-to-point-mac parameter ... 6-16
  RSTP priority parameter ... 6-16
  rules, operating, fast-uplink ... 6-32
  viewing the configuration ... 6-12
  VLAN effect on ... 2-51
  with 802.1Q VLANs ... 6-7
spanning tree protocol
  See STP.
spanning-tree, 802.1s ... 6-3, 6-44
  802.1D and 802.1w connections ... 6-52
  802.1D as a region ... 6-51, 6-52
  802.1D connection requirement ... 6-61
  802.1Q VLANs ... 6-49
  802.1s standard-compliant ... 6-44
  802.1w as a region ... 6-51
  activation ... 6-58
  active path ... 6-48
  active paths ... 6-52
  bandwidth loss ... 6-49
  benefit ... 6-44
  blocked traffic ... 6-49
  boundary port, region ... 6-51, 6-52
  boundary port, VLAN membership ... 6-49
  BPDU ... 6-49, 6-55, 6-59, 6-60, 6-61
  BPDU requirement ... 6-51
  BPDU, function ... 6-51
  bridge ... 6-51
  bridge, designated for region ... 6-51
  caution ... 6-44, 6-47
  CIST ... 6-45, 6-50, 6-52
  CIST per-port hello time ... 6-52
  CIST root ... 6-62
  common and internal spanning tree
    See CIST.
  common spanning tree
    See CST.
  compatibility ... 6-53
  compatibility mode ... 6-60
  configuration ... 6-57, 6-69
  configuration identifier ... 6-51
  configuration steps ... 6-55
  configuration, exchanging ... 6-69
  configuration, MST instance ... 6-63
  configuration, MSTI per-port ... 6-66
  configuration, port ... 6-61
  convergence time, minimize ... 6-58
  CST ... 6-45, 6-49, 6-51
  CST and legacy devices ... 6-49
  CST, view status ... 6-71, 6-72
  default configuration ... 6-47
  designated bridge ... 6-49, 6-51
  designated port ... 6-49
  disabling MSTP ... 6-69
  display statistics and configuration ... 6-71
  dynamic VLANs, disallowed ... 6-46
  edge port ... 6-61
enabling a region ... 6-69
enabling MSTP ... 6-69
example of multiple topologies ... 6-48
fault tolerance ... 6-44
force protocol version ... 6-53
force-version ... 6-61
forwarding paths ... 6-53
forwarding state ... 6-61
frame duplication and misordering ... 6-53
general operation ... 6-3, 6-44
GVRP ... 6-46, 6-53
hello-time, CIST root, propagated ... 6-52, 6-60
hello-time, override ... 6-52
hello-time, propagated ... 6-52
hop-count decremented ... 6-59
instance ... 6-3, 6-52, 6-56
instance, forwarding topology ... 6-52
instance, IST ... 6-46
instance, type ... 6-46
internal spanning tree
See IST.
interoperating with 802.1D and 802.1w ... 6-51
IST ... 6-46
IST instance ... 6-46, 6-63
IST root ... 6-46, 6-48, 6-51
IST, defined ... 6-51
IST, dynamic VLAN ... 6-53
IST, root switch ... 6-51
IST, switch membership ... 6-51
IST, VLAN membership ... 6-46
legacy devices and the CST ... 6-49
legacy STP and RSTP ... 6-49
mesh environment ... 6-44, 6-53
MIB ... 6-78
MST region
See region.
MSTI ... 6-46, 6-52
MSTI root ... 6-48
MSTI, view status ... 6-73
MSTP ... 6-47
MSTP operation ... 6-47
MSTP, view global configuration ... 6-74
multiple spanning tree instance
See MSTI
override hello-time ... 6-52
path cost, effect on 802.1D ... 6-53
pending configuration ... 6-77
pending option ... 6-47, 6-59, 6-69, 6-70
per-VLAN STP ... 6-44
planning ... 6-54
port connectivity ... 6-61
port states ... 6-48, 6-53
priority resolution ... 6-64
priority, device ... 6-56, 6-65
priority, IST port ... 6-68
priority, MSTI port ... 6-67
rapid state transitions ... 6-53, 6-55
redundant links ... 6-49
region ... 6-3, 6-45, 6-46
region name ... 6-51, 6-58
region root switch ... 6-46
region, configuration name ... 6-78
region, Configuration Revision number ... 6-78
region, defined ... 6-51
region, enabling ... 6-69
region, root bridge ... 6-50
region, RSTP bridge ... 6-52
region, switch configuration ... 6-52
region, switch excluded ... 6-78
region, view configuration ... 6-76
region, VLAN assignments ... 6-51
regional boundary port ... 6-51
regional root bridge per-instance ... 6-49
regional root switch ... 6-51
regional root switch, configuration ... 6-52
regions, communication between ... 6-52
root bridge ... 6-45
root bridge per-instance ... 6-49
root bridge per-region ... 6-50
root port per-instance ... 6-49
root switch, instance ... 6-64
root switch, IST instance ... 6-46, 6-51
root switch, MST instance ... 6-52
root switch, regional ... 6-51, 6-52
root, CIST ... 6-60
root, IST ... 6-51
root, MSTI ... 6-48
routed traffic in a region ... 6-49
RSTP as a region ... 6-45
RSTP BPDU requirement ... 6-51
RSTP bridge ... 6-52
rules for operation ... 6-52
separate forwarding paths ... 6-46
show commands ... 6-71
SNMP MIB ... 6-78
STP as a region ... 6-45
Index – 13
switch excluded from region ... 6-78
 topology between regions ... 6-47
 trunk, root, per-instance ... 6-49
 trunked link ... 6-74
 trunked link example ... 6-50
 types of MST instances ... 6-46
 VLAN assignments, region ... 6-51, 6-52
 VLAN membership, region ... 6-50
 VLAN, change instance ... 6-56
 VLAN, configuration error ... 6-78
 VLAN, connectivity between regions ... 6-52
 VLAN, duplicate or missing packets ... 6-78
 VLAN, dynamic ... 6-46
 VLAN, instance assigned ... 6-48, 6-52, 6-63
 with legacy STP and RSTP ... 6-45
 static IP routes
 configuring ... 10-17, 10-19
 IP routing
 static route parameters ... 10-18
 route types ... 10-17
 static NAT
 See routing.
 static routes
 affect of XRRP ... 11-9
 static VLAN, convert to ... 3-3
 statistics
 XRRP ... 11-19
 status and counters
 XRRP ... 11-18
 STP
 cost change by mesh switch ... 7-21
 enabling from the CLI ... 6-13
 server access failure ... 6-6
 stub area
 OSPF ... 10-41
 subnet ... 2-3, 4-12
 subnet address ... 2-6
 supernetting ... 9-21
 supersede implicit deny any ... 9-27
 switch meshing
 See mesh.
 Syslog
 See ACL, logging.

T
 tables
 ARP cache ... 10-5
 IP ... 10-4
 IP route ... 10-5
terminology
 XRRP ... 11-2
ToS
 See Class of Service.
transit area
 OSPF ... 10-45
 trap
 OSPF ... 10-51
 XRRP ... 11-18
 trunk, spanning-tree example ... 6-50
 Type of Service
 using to prioritize IP traffic ... 8-24
 Type of Service field (IP)
 configuring packet priority ... 8-24
 how the switch uses it ... 8-35
 Type, meshed port ... 7-12

U - V
 unicast in switch mesh ... 7-19
 upstream device QoS)
 definition ... 8-5
 VID
 See VLAN.
 Viewing
 spanning tree configuration ... 6-12
 virtual link
 OSPF ... 10-45
 displaying information ... 10-66
 parameters ... 10-47
 virtual neighbor
 OSPF
 displaying information ... 10-65
 virtual router, XRRP
 definition ... 11-2
 VLAN ... 2-52
 802.1Q ... 6-7
 assigning OSPF area to ... 10-43
 broadcast domain ... 2-3
 CLI, commands ... 2-28
 CLI, configuring parameters ... 2-27
 convert dynamic to static ... 2-34, 3-3
 dedicated management ... 2-43
 DEFAULT_VLAN ... 2-43
 deleting ... 2-53
 DHCP, primary VLAN ... 2-43
configuration
  multiple VLAN example … 11-17
  single VLAN example … 11-16
configuration examples … 11-16
configuration rules … 11-15
configuring … 11-11
configuring interfaces … 11-13
displaying status and data … 11-18
dynamic reconfiguration … 11-15
enabling and disabling … 11-15
fail-over operation … 11-5
  fast fail-over … 11-7
  multiple VLANs … 11-6
  single VLAN … 11-5
  standard fail-over … 11-8
  total router fail-over … 11-6
introduction … 11-2
master … 11-2
multiple forwarding database … 11-10
  multiple VLANs … 11-10
normal router operation … 11-4
operation notes … 11-9
overview of operation … 11-3
owner … 11-2
peer router connectivity requirements … 11-10
Protection Domain … 11-2
show statistics … 11-19
show traps … 11-18
terminology … 11-2
virtual router … 11-2
xrrp command
  domain parameter … 11-12
  failback parameter … 11-13
  instance parameter … 11-13
  router parameter … 11-12
  syntax … 11-12
  trap parameter … 11-13

X
XRRP
  advertisement interval … 11-2
    configuring … 11-14
  affect on proxy ARP … 11-9
  affect on static and default routes … 11-9
  authentication
    configuring … 11-14
  CLI command … 11-12
  CLI commands
    domain … 11-12
    failback … 11-13
    instance … 11-13
    router … 11-12
    trap … 11-13
  compared with VRRP … 11-21

X

xrrp command
  domain parameter … 11-12
  failback parameter … 11-13
  instance parameter … 11-13
  router parameter … 11-12
  syntax … 11-12
  trap parameter … 11-13

W
warranty … 1-ii
web browser interface
  enabling RSTP … 6-20
web browser interface, for configuring
  IGMP … 4-11
  Quality of Service … 8-56
  STP … 6-43
wildcard
  See ACL.
wildcard, ACL, defined … 9-7
write memory … 3-18