Abstract

Applicable Products

HP Switch 3800–24 (J9470A)
HP Switch 3800–48 (J9472A)
HP Switch 3800-24-PoE (J9471A)
HP Switch 3800–48-PoE (J9473A)
HP Switch 3800yl-24G-PWR (J8692A)
HP Switch 3800yl-48G-PWR (J8693A)
HP Switch 3800–24G-PoE+-2SFP+ (J9573A)
HP Switch 3800–48G-PoE+-4SFP+ (J9574A)
HP Switch 3800–24G-2SFP+ (J9575A)
HP Switch 3800–48G-4SFP+ (J9576A)
HP Switch 3800–24GS-2XG tl (J9584A)
HP Switch 3800–24G-2XGT tl (J9585A)
HP Switch 3800–48G-4XGT tl (J9586A)
HP Switch 3800–24G-2XGT-PoE+ tl (J9587A)
© Copyright 2008, 2012 Hewlett-Packard Development Company, L.P.
Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor’s standard commercial license. The information contained herein is subject to change without notice. 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. UNIX is a registered trademark of The Open Group.

Acknowledgments
Microsoft, Windows, Windows XP, and Windows NT are U.S. registered trademarks of Microsoft Corporation.
Java and Oracle are registered trademarks of Oracle and/or its affiliates.

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

## 1 Multimedia Traffic Control with IP Multicast (IGMP)

- Overview..............................................................................................................16
- Enabling IGMP....................................................................................................16
- Configuring and displaying IGMP (CLI).............................................................16
  - Viewing IGMP configuration for VLANs.........................................................16
  - Viewing the current IGMP configuration.......................................................17
  - Viewing IGMP high level statistics for all VLANs on the switch....................18
  - Viewing IGMP historical counters for a VLAN..............................................19
  - Viewing IGMP group address information....................................................19
  - Viewing IGMP group information for a VLAN with a filtered address..........20
- Enabling or disabling IGMP on a VLAN..........................................................20
- Configuring per-port IGMP traffic filters.........................................................21
- Configuring the querier function.......................................................................22
- Configuring the querier interval.........................................................................22
- Configuring static multicast groups....................................................................22
- Configuring fast-leave IGMP...............................................................................23
- Configuring forced fast-leave IGMP ....................................................................23
- Configuring fast learn .......................................................................................23
- Configuring delayed group flush .......................................................................23
- Preventing unjoined multicast traffic...............................................................24
- Configuring IGMP proxy (CLI)..........................................................................24
  - Adding or leaving a multicast domain.............................................................24
  - Informs the VLAN which IGMP proxy domains to use with joins on the VLAN..25
- Viewing the IGMP proxy data..........................................................................25
- IGMP general operation and features...............................................................26
- Enhancements......................................................................................................27
- Number of IP multicast addresses allowed.......................................................27
- How IGMP operates.........................................................................................27
  - Operation with or without IP addressing......................................................28
  - Automatic fast-leave IGMP............................................................................29
  - Default (enabled) IGMP operation solves the "delayed leave" problem...........30
  - Forced fast-leave IGMP..................................................................................31
  - Fast learn .......................................................................................................31
  - Unjoined multicast traffic.............................................................................31
  - IGMP proxy forwarding................................................................................33
    - How IGMP proxy forwarding works...........................................................34
    - Operating notes for IGMP proxy forwarding..............................................34
- About using the switch as querier......................................................................36
- Well-known or reserved multicast addresses excluded from IP multicast filtering.37
- IP multicast filters............................................................................................37
  - Reserved addresses excluded from IP multicast (IGMP) filtering....................37

## 2 PIM-DM (Dense Mode)

- Overview..............................................................................................................38
- Global and PIM configuration contexts.............................................................40
  - Enabling or disabling IP multicast routing....................................................40
  - Enabling or disabling PIM at the global level; placing the CLI in the PIM context.40
  - Setting the interval in seconds between successive state-refresh messages originated by the routing switch.........................................................40
- Enabling and disabling PIM SNMP traps...........................................................40
- PIM VLAN (interface) configuration context...................................................42
  - Enabling multicast routing on the VLAN interface to which the CLI is currently set.42

---

*Note: The contents are extracted from the beginning of the document, and the page numbers are placeholders.*
Specifying the IP address to use as the source address for PIM protocol packets outbound on the VLAN...........................................43
Changing the frequency at which the routing switch transmits PIM hello messages on the current VLAN..................................................43
Changing the maximum time in seconds before the routing switch actually transmits the initial PIM hello message on the current VLAN..................................................44
Changing the interval the routing switch waits for the graft ack from another router before resending the graft request..................................................44
Changing the number of times the routing switch retries sending the same graft packet to join a flow..................................................44
Enabling the LAN prune delay option on the current VLAN...........................................45
Computing the lan-prune-delay setting........................................................................45
Setting the multicast datagram time-to-live (router hop-count) threshold for the VLAN...........................................46
Example of configuring PIM-DM operation at the VLAN level...........................................46
Displaying PIM data and configuration settings...........................................48
Displaying PIM route data........................................................................48
Displays the PIM interfaces currently configured...........................................49
Viewing VLAN, protocol identity, and TTL settings.........................................49
Viewing data for a specified flow (multicast group)...........................................50
Displaying PIM status................................................................................52
Displaying PIM neighbor data........................................................................52
Variation........................................................................53
Listing the PIM interfaces (VLANs) currently configured in the routing switch...........................................53
Viewing the current configuration for the specified VLAN (PIM interface)...........................................54
Viewing PIM-specific information from the IP multicast routing table (MRT)...........................................55
Viewing the PIM route entry information for the specified multicast group (flow)...........................................55
Listing PIM neighbor information for all PIM neighbors connected to the routing switch...........................................56
About PIM-DM...........................................57
PIM-DM features........................................................................58
PIM-DM operation........................................................................58
Multicast flow management........................................................................60
Initial flood and prune........................................................................60
Maintaining the prune state........................................................................60
State-refresh packets and bandwidth conservation...........................................60
General configuration elements........................................................................61
About configuring PIM-DM........................................................................61
Operating notes........................................................................62
PIM-DM operating rules........................................................................62
PIM routers without state-refresh messaging capability...........................................62
Flow capacity........................................................................62
IGMP traffic high-priority disabled........................................................................62
ACLs and PIM........................................................................62
When to enable IGMP on a VLAN........................................................................62
IP address removed........................................................................62
Troubleshooting........................................................................63
Symptom: Noticeable slowdown in some multicast traffic...........................................63
Heavy memory usage........................................................................63
IPv4 table operation........................................................................63
Messages related to PIM operation........................................................................63
Applicable RFCs........................................................................66
Exceptions to Support for RFC 2932 - Multicast Routing MIB...........................................66
3 PIM-SM (Sparse Mode)........................................................................68
Configuring router protocol independent multicast (PIM)...........................................70
Configuring PIM-SM on the router........................................................................71
Global configuration context for supporting PIM-SM...............................................................71
Configuring global context commands.....................................................................................71
VLAN context commands for configuring PIM-SM........................................................................74
Enabling or disabling IGMP in a VLAN......................................................................................74
Enabling or disabling PIM-SM per-VLAN..................................................................................74
Changing the interval for PIM-SM neighbor notification.............................................................74
Changing the randomized delay setting for PIM-SM neighbor notification..............................75
Enabling or disabling lan prune delay.......................................................................................75
Changing the lan-prune-delay interval......................................................................................76
Neighbor timeout......................................................................................................................76
Changing the DR priority..........................................................................................................76
Configuring PIM-SM support in a VLAN context........................................................................76
Router PIM context commands for configuring PIM-SM operation............................................77
Configuring a BSR candidate....................................................................................................77
Enabling or disabling a BSR Candidate...................................................................................77
Changing the priority setting.....................................................................................................78
Changing the distribution...........................................................................................................78
Changing the message interval....................................................................................................78
Configuring C-RPs on PIM-SM routers......................................................................................79
  Specifying the source IP VLAN (and optionally configuring one or more multicast groups or range
  of groups)...............................................................................................................................79
  Enabling or disabling C-RP operation......................................................................................81
  Adding or deleting a multicast group address..........................................................................81
  Changing the C-RP hold-time...............................................................................................82
  Changing a C-RP's election priority.......................................................................................82
Enabling, disabling, or changing router PIM notification traps..............................................82
Changing the global join-prune interval on the router..........................................................83
Changing the shortest-path tree (SPT) operation......................................................................83
Statically configuring an RP to accept multicast traffic.........................................................83
  Configuring PIM-SM support in the router PIM context.........................................................84
Configuring PIM RPF override...............................................................................................85
Displaying configured RPF overrides......................................................................................86
Displaying PIM route data.........................................................................................................86
  Listing basic route data for active multicast groups.............................................................86
  Listing data for an active multicast group..........................................................................88
  Listing all VLANs having currently active PIM flows........................................................91
Displaying PIM-specific data......................................................................................................91
  Displaying the current PIM status and global configuration...............................................92
  Displaying current PIM entries existing in the multicast routing table...................................92
  Listing currently configured PIM interfaces.......................................................................93
  Displaying IP PIM VLAN configurations ..........................................................................93
Displaying PIM neighbor data..................................................................................................94
Display pending join requests.................................................................................................95
Displaying BSR data................................................................................................................96
  Displaying BSR status and configuration............................................................................96
  Listing non-default BSR configuration settings...................................................................97
Displaying the current RP set....................................................................................................98
Displaying C-RP data...............................................................................................................99
  Displaying the router's C-RP status and configuration...........................................................99
  Listing non-default C-RP configuration settings...................................................................100
PIM-SM overview.....................................................................................................................101
PIM-SM features.......................................................................................................................101
PIM-SM operation and router types........................................................................................102
  Pim-SM operation...............................................................................................................102
  Rendezvous-point tree (RPT).............................................................................................102
Routing Basics........................................................................................116
Enabling proxy ARP..............................................................................................................118
Increasing ARP age timeout (CLI)............................................................................................116
Reconfiguring the router ID (optional)......................................................................................118
Operating rules and recommendations....................................................................................109
Pim-SM router types..............................................................................................................114
DR.................................................................................................................................105
BSR..................................................................................................................................105
BSR configuration and election............................................................................................105
BSR role in fault recovery.................................................................................................106
RP..................................................................................................................................106
Defining supported multicast groups....................................................................................106
C-RP election..................................................................................................................107
Redundant Group Coverage Provides Fault-Tolerance.........................................................107
Static RP (static RP)...........................................................................................................107
General application........................................................................................................107
Supporting a static RP as primary....................................................................................108
Operating rules for static RPs..........................................................................................108
Configuration................................................................................................................109
Operating rules and recommendations..................................................................................109
Configuration steps for PIM-SM..........................................................................................109
Planning considerations....................................................................................................109
Per-router global configuration context.................................................................................110
Per-VLAN PIM-SM configuration.......................................................................................110
Router Pim configuration...................................................................................................111
Operating notes...............................................................................................................112
Event log messages..........................................................................................................113

4 Routing Basics.................................................................................................116
Viewing the IP route table...................................................................................................116
Increasing ARP age timeout (CLI)........................................................................................116
Setting and viewing the arp-age value (Menu)........................................................................117
Reconfiguring the router ID (optional)................................................................................118
Changing the router ID........................................................................................................118
Enabling proxy ARP..........................................................................................................118
Enabling local proxy ARP..................................................................................................119
Enabling forwarding of IP directed broadcasts (CLI)..............................................................119
Disabling the directed broadcasts......................................................................................120
Disabling replies to broadcast ping requests........................................................................120
Disabling all ICMP unreachable messages..........................................................................120
Disabling ICMP redirects..................................................................................................120
Overview of IP routing.......................................................................................................120
IP interfaces....................................................................................................................121
IP tables and caches...........................................................................................................121
ARP cache table................................................................................................................121
ARP cache.......................................................................................................................121
IP route table....................................................................................................................122
Routing paths....................................................................................................................122
Administrative distance......................................................................................................122
IP forwarding cache..........................................................................................................123
IP route exchange protocols..............................................................................................123
IP global parameters for routing switches........................................................................123
IP interface parameters for routing switches.....................................................................125
Configuring IP parameters for routing switches................................................................126
Configuring IP addresses....................................................................................................126

Contents
Assigning loopback addresses to an area (optional).................................................................158
OSPF redistribution of loopback addresses................................................................................159
Configuring external route redistribution in an OSPF domain (optional).................................160
Configuring redistribution filters............................................................................................160
Enabling route redistribution....................................................................................................161
Modifying the default metric for redistribution (optional)........................................................161
Modifying the redistribution metric type (optional)....................................................................162
Configuring ranges on an ABR to reduce advertising to the backbone (optional)......................162
Assigning a cost........................................................................................................................163
Allowing or blocking advertisement of a range of internal routes available in an area by an ABR................................................................................................................................................164
Allowing or blocking a range of external routes available through an ASBR in an NSSA..............165
Influencing route choices by changing the administrative distance default (optional)................165
Changing OSPF trap generation choices (optional).......................................................................165
Adjusting performance by changing the VLAN or subnet interface settings (optional).............166
Indicating the cost per-interface.................................................................................................167
Indicating the per-interface dead interval....................................................................................167
Indicating the per-interface hello interval...................................................................................167
Changing priority per-interface....................................................................................................168
Changing retransmit interval per-interface..................................................................................168
Changing transit-delay per-interface............................................................................................168
Examples of changing per-interface settings..................................................................................169
Configuring OSPF interface authentication (optional)...................................................................169
Configuring OSPF password authentication..................................................................................169
Configuring OSPF MD5 authentication........................................................................................170
Configuring a virtual link...........................................................................................................171
Changing the dead interval on a virtual link................................................................................172
Indicating the hello interval on a virtual link................................................................................172
Changing the retransmitting interval on a virtual link..................................................................173
Changing the transit-delay on a virtual link..................................................................................173
Configuring OSPF authentication on a virtual link......................................................................174
Authenticating the OSPF password on a virtual link..................................................................174
Authenticating OSPF MD5 on a virtual link..................................................................................175
Configuring a passive OSPF interface..........................................................................................175
Configuring the calculation interval............................................................................................176
Viewing OSPF information...........................................................................................................177
Viewing general OSPF configuration information........................................................................177
Viewing OSPF area information..................................................................................................179
Viewing OSPF external link-state information.............................................................................180
Viewing OSPF interface information.............................................................................................181
Viewing OSPF interface information for a specific VLAN or IP address.................................182
Viewing OSPF packet statistics for a subnet or VLAN.................................................................183
Clearing OSPF statistics for all VLAN interfaces on the switch....................................................185
Viewing OSPF link-state information............................................................................................185
Viewing OSPF neighbor information..................................................................................................190
Viewing OSPF redistribution information..................................................................................191
Viewing OSPF redistribution filter (restrict) information.............................................................192
Viewing OSPF virtual neighbor information....................................................................................192
Viewing OSPF virtual link information..........................................................................................193
Viewing OSPF SPF statistics..........................................................................................................194
Displaying OSPF route information............................................................................................195
Viewing OSPF traps enabled..........................................................................................................197
Debugging OSPF routing messages................................................................................................197
Enabling load sharing among next-hop routes...............................................................................197
Viewing the current IP load-sharing configuration.......................................................................198
Overview of OSPF............................................................................................................................198
OSPF router types ..........................................................................................................................199
  Interior routers .......................................................................................................................199
  Area border routers (ABRs) ..................................................................................................200
  Autonomous system boundary router (ASBR) ..................................................................200
  Designated routers (DRs) .....................................................................................................200
OSPF area types ...........................................................................................................................202
  Backbone area .......................................................................................................................202
  Normal area ...........................................................................................................................203
  Not-so-stubby-area (NSSA) ..................................................................................................203
  Stub area ................................................................................................................................203
OSPF RFC compliance ................................................................................................................204
Reducing AS external LSAs and Type-3 summary LSAs ............................................................204
  Algorithm for AS external LSA reduction .............................................................................204
  Replacing type-3 summary LSAs and type-7 default external LSAs with a type-3 default route
  LSA ........................................................................................................................................205
Equal cost multi-path routing (ECMP) ..........................................................................................205
Dynamic OSPF activation and configuration ..............................................................................207
  General configuration steps for OSPF ....................................................................................208
    Configuration rules .............................................................................................................208
    OSPF global and interface settings ...................................................................................209
Changing the RFC 1583 OSPF compliance setting ......................................................................209
Assigning the routing switch to OSPF areas ................................................................................209
Configuring for external route redistribution in an OSPF domain ............................................210
Configuring ranges on an ABR to reduce advertising to the backbone (optional) ......................210
Influencing route choices by changing the administrative distance default (optional) ...............210
Adjusting performance by changing the VLAN or subnet interface settings (optional) ..........211
Configuring OSPF interface authentication (optional) ..................................................................211
Configuring an ABR to use a virtual link to the backbone ........................................................211
Adjusting virtual link performance by changing the interface settings (optional) .....................212
Configuring OSPF authentication on a virtual link .....................................................................212
About OSPF passive ....................................................................................................................212
About configuring shortest path first (SPF) scheduling .............................................................212
Graceful shutdown of OSPF routing ............................................................................................213
  Modules operating in nonstop mode ......................................................................................213
  OSPF equal-cost multipath (ECMP) for different subnets available through the same next-hop
  routes ......................................................................................................................................213

8 Route Policy ............................................................................................................................215
Using prefix lists ..........................................................................................................................215
  Creating prefix list entries ......................................................................................................216
  Entering a prefix list description ...............................................................................................217
  Viewing prefix lists ....................................................................................................................218
Creating a route map ....................................................................................................................219
  Deleting all or part of a route map ..........................................................................................219
  Viewing route maps ..................................................................................................................220
Using match commands ..............................................................................................................220
  Matching VLANs ......................................................................................................................220
  Matching prefix lists ................................................................................................................220
  Matching next-hop addresses .................................................................................................221
  Matching route sources .........................................................................................................221
  Matching route metrics .........................................................................................................221
  Matching metric types ..........................................................................................................221
  Matching source protocols ....................................................................................................222
  Matching tags ..........................................................................................................................222
Using set commands..............................................................................................................222
Setting the next hop..............................................................................................................222
Setting the route metric........................................................................................................223
Setting the metric type.........................................................................................................223
Setting the tag value..............................................................................................................223
Route policy overview..............................................................................................................223
Configuring route policy........................................................................................................224
Route maps................................................................................................................................224
Match commands..................................................................................................................225
Using route policy in route redistribution...........................................................................225
Baseline: Intra-domain routing using default settings.........................................................226
Basic inter-domain protocol redistribution..........................................................................229
Finer control of inter-domain routing using route policy....................................................230
Redistribution using tags.......................................................................................................234

9 ICMP Router Discovery Protocol........................................................................................237
Configuring IRDP..................................................................................................................237
Enabling IRDP globally..........................................................................................................237
Enabling IRDP on an individual VLAN interface...................................................................238
Viewing IRDP information.....................................................................................................239

10 Dynamic Host Configuration Protocol.............................................................................240
Enabling DHCP relay............................................................................................................240
Using DHCP Option 12 to send a hostname........................................................................241
Configuring a BOOTP/DHCP relay gateway......................................................................241
Viewing the BOOTP gateway...............................................................................................242
Operating notes......................................................................................................................242
Configuring an IP helper address.........................................................................................243
Operating notes......................................................................................................................243
Disabling the hop count in DHCP requests..........................................................................243
Operating notes......................................................................................................................243
Verifying the DHCP relay configuration...............................................................................243
Viewing the DHCP relay setting..........................................................................................243
Viewing DHCP helper addresses..........................................................................................244
Viewing the hop count setting..............................................................................................244
Viewing the MAC address for a routing switch...................................................................245
Configuring Option 82..........................................................................................................245
Operating notes......................................................................................................................248
Overview of DHCP................................................................................................................249
DHCP packet forwarding......................................................................................................249
Unicast forwarding................................................................................................................249
Broadcast forwarding..........................................................................................................249
Enabling DHCP relay operation..........................................................................................249
Hop count in DHCP requests..............................................................................................249
DHCP Option 82....................................................................................................................249
Option 82 server support.......................................................................................................250
General DHCP Option 82 requirements and operation.......................................................251
Requirements.......................................................................................................................251
General DHCP-relay operation with Option 82...................................................................251
Option 82 field content..........................................................................................................251
Forwarding policies..............................................................................................................252
Multiple Option 82 relay agents in a client request path....................................................254
Validation of server response packets................................................................................255
Multinetted VLANs..............................................................................................................257
11 User Datagram Protocol.................................................................258
Configuring and enabling UDP broadcast forwarding..........................258
Globally enabling UDP broadcast forwarding.........................................258
Configuring UDP broadcast forwarding on individual VLANs.................258
Viewing the current IP forward-protocol configuration............................259
Operating notes for UDP broadcast forwarding........................................260
Maximum number of entries.......................................................................260
TCP/UDP port number ranges......................................................................261
Messages related to UDP broadcast forwarding.........................................261
UDP broadcast forwarding..........................................................................261
Subnet masking for UDP forwarding addresses..........................................262

12 Virtual Router Redundancy Protocol (VRRP)........................................263
VRRP overview.......................................................................................264
Configuring VRRP...................................................................................265
Enabling VRRP in the global configuration context.................................265
Creating a VR and entering the VR context.............................................266
Configuring a VR instance on a VLAN interface......................................266
Assigning owner and backup status.........................................................266
Configuring a virtual IP address (VIP) in a VR.........................................267
Reconfiguring the priority for a backup....................................................268
Changing VR advertisement interval and source IP address......................268
Configuring preempt mode on VRRP backup routers...............................269
Enabling or disabling VRRP operation on a VR.........................................269
Dynamically changing the priority of the VR..............................................270
Configuring track interface......................................................................270
Configuring track VLAN.........................................................................270
Removing all tracked entities....................................................................271
Forcing the backup VR operating as master to relinquish ownership of the VR instance..................................................271
Forcing the backup VR to take ownership of the VR instance.....................271
Viewing VRRP tracked entities.................................................................271
Pinging the virtual IP of a backup router..................................................271
Enabling the response to a ping request..................................................271
Controlling ping responses.......................................................................272
Viewing VRRP ping information...............................................................273
Operational notes......................................................................................276
Specifying the time a router waits before taking control of the VIP.............276
Viewing VRRP configuration data.............................................................276
Viewing the VRRP global configuration....................................................276
Viewing all VR configurations on the router.............................................277
Viewing a specific VR configuration.........................................................278
Viewing VRRP statistics data....................................................................279
Viewing global VRRP statistics only.........................................................279
Viewing statistics for all VRRP instances on the router............................280
Viewing statistics for all VRRP instances in a VLAN..................................282
Viewing statistics for a specific VRRP instance........................................283
Viewing the "near-failovers" statistic.........................................................283
Using the debug command with the VRRP option....................................284
General operation...................................................................................284
Virtual router (VR)................................................................................286
Virtual IP address (VIP)...........................................................................287
Master router..........................................................................................287
Control of master selection......................................................................287
Function of the VRRP advertisement......................................................287
Owner router..........................................................................................287

Contents 11
13 Border Gateway Protocol (BGP) ......................................................... 300

Global BGP configuration ................................................................. 300
    Configuring a BGP routing process ........................................... 300
    Configuring a fixed router ID for local BGP routing process ..... 300
    Specifying the networks to be advertised by BGP routing process .................................................. 301
    Adjusting BGP network timers ................................................. 301
    Re-enabling state contained within nodes of BGP processes .................................................................. 301

Global BGP policy configuration ..................................................... 301
    Delaying sending the BGP open message ................................. 303
    Maximum routes that BGP will accept for installation into RIB ................................................................. 303
    Enabling comparison of MED for paths from neighbors in different autonomous systems ..................... 303
    Specifying number of times an AS number can appear in AS_PATH ..................................................... 303
    Configuring BGP to not consider AS_PATH ............................... 304
    Breaking ties between routes based on originator ID value ................................................................. 304
    Comparing identical routes received from different external peers ......................................................... 304
    Assigning value of infinity to routes missing MED attribute ................................................................... 304
    Setting BGP MED on routes when advertised to peers ........................................................................... 304
    Specifying a route’s preference .................................................. 305
    Enabling client-to-client route reflection ................................................................................................. 305
    Specifying BGP cluster ID when BGP router is route-reflector .................................................................. 305

BGP graceful restart ................................................................. 305
    Configuring BGP graceful restart timers .................................... 306
    Enabling event logging ............................................................. 306
### Table 1 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip igmp [vlan vid]</td>
<td>Displays IGMP configuration for a specified VLAN or for all VLANs on the switch.</td>
<td>-</td>
<td>(page 16)</td>
<td>-</td>
</tr>
<tr>
<td>show ip igmp config</td>
<td>Displays IGMP configuration for all VLANs on the switch.</td>
<td>-</td>
<td>(page 17)</td>
<td>-</td>
</tr>
<tr>
<td>show ip igmp statistics</td>
<td>Displays IGMP high level statistics for all VLANs on the switch.</td>
<td>-</td>
<td>(page 18)</td>
<td>-</td>
</tr>
<tr>
<td>show ip igmp vlan vid counters</td>
<td>Displays IGMP historical counters for a VLAN.</td>
<td>-</td>
<td>(page 19)</td>
<td>-</td>
</tr>
<tr>
<td>show ip igmp groups</td>
<td>Displays IGMP group address information.</td>
<td>-</td>
<td>(page 19)</td>
<td>-</td>
</tr>
<tr>
<td>show ip igmp vlan vid group ip-addr</td>
<td>Displays IGMP group information for a VLAN with a filtered address.</td>
<td>-</td>
<td>(page 20)</td>
<td>-</td>
</tr>
<tr>
<td>show ip igmp vlan vid config</td>
<td>Displays IGMP configuration for a specific VLAN on the switch, including per-port data.</td>
<td>-</td>
<td>(page 17)</td>
<td>-</td>
</tr>
<tr>
<td>vlan vid ip igmp [ auto port-list</td>
<td>blocked port-list</td>
<td>forward port-list ]</td>
<td>Used in the VLAN context, specifies how each port should handle IGMP traffic.</td>
<td>auto</td>
</tr>
<tr>
<td>[no] vlan vid ip igmp querier</td>
<td>Disables or re-enables the ability for the switch to become querier if necessary.</td>
<td>enabled</td>
<td>(page 22)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip igmp querier interval [5-300]</td>
<td>Specifies number of seconds between membership queries.</td>
<td>125 seconds</td>
<td>(page 22)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip igmp static-group group-address</td>
<td>Configures a group on the switch so that multicast traffic for that group can be forwarded with a receiver host.</td>
<td>-</td>
<td>(page 22)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip igmp fastleave port-list</td>
<td>Enables IGMP fast-leaves on the specified VLAN.</td>
<td>-</td>
<td>(page 23)</td>
<td>-</td>
</tr>
<tr>
<td>[no] igmp filter-unknown-mcast</td>
<td>Enables interface isolation for unjoined multicast groups.</td>
<td>disabled</td>
<td>(page 31)</td>
<td>-</td>
</tr>
<tr>
<td>[no] vlan vid ip igmp forcedfastleave port-list</td>
<td>Enables IGMP forced fast-leave on the specified ports in the selected VLAN, even if they are cascaded.</td>
<td>disabled</td>
<td>(page 23)</td>
<td>-</td>
</tr>
<tr>
<td>[no] igmp fastlearn port-list</td>
<td>Enables fast learn on the specified ports.</td>
<td>disabled</td>
<td>“Configuring fast learn” (page 23)</td>
<td>-</td>
</tr>
<tr>
<td>igmp delayed-flush time-period</td>
<td>Where leaves have been sent for IGMP groups, enables the switch to continue to flush the</td>
<td>disabled</td>
<td>(page 23)</td>
<td>-</td>
</tr>
</tbody>
</table>
**Overview**

This chapter describes multimedia traffic control with IP multicast—Internet Group Management Protocol (IGMP) controls—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 about IGMP, see “IGMP general operation and features” (page 26).

**NOTE:** The use of static multicast filters is described in the chapter titled “Traffic/Security Filters” in the Access Security Guide for your HP switch.

**Enabling IGMP**

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

- If multiple VLANs are not configured:
  Configure IGMP on the default VLAN (DEFAULT_VLAN; VID=1).

- If multiple VLANs are configured:
  Configure IGMP on a per-VLAN basis for every VLAN where this feature is to be used.

**Configuring and displaying IGMP (CLI)**

**Viewing IGMP configuration for VLANs**

Syntax:

```
show ip igmp [vlan vid]
```

Displays IGMP configuration for a specified VLAN or for all VLANs on the switch.
**Example**

**Example 1 Displaying IGMP status for a VLAN**

HP Switch(config)# show ip igmp vlan 1

**IGMP Service Protocol Info**

<table>
<thead>
<tr>
<th>Total VLANs with IGMP enabled:</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current count of multicast groups joined:</td>
<td>20</td>
</tr>
<tr>
<td>VLAN ID:</td>
<td>2</td>
</tr>
<tr>
<td>VLAN Name:</td>
<td>VLAN2</td>
</tr>
<tr>
<td>IGMP version:</td>
<td>2</td>
</tr>
<tr>
<td>Querier Address:</td>
<td>10.255.128.2</td>
</tr>
<tr>
<td>Querier Port:</td>
<td>A1</td>
</tr>
<tr>
<td>Querier UpTime:</td>
<td>1h 51m 59s</td>
</tr>
<tr>
<td>Querier Expiration Time:</td>
<td>2min 5sec</td>
</tr>
<tr>
<td>Ports with multicast routers:</td>
<td>A1, A5-A6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Active Group Addresses</th>
<th>Type</th>
<th>Expires</th>
<th>Ports</th>
<th>Reports</th>
<th>Queries</th>
</tr>
</thead>
<tbody>
<tr>
<td>226.0.6.7</td>
<td>Filter</td>
<td>2min 5sec</td>
<td>A1</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>226.0.6.8</td>
<td>Standard</td>
<td>3min 20sec</td>
<td>A2</td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>

**Viewing the current IGMP configuration**

**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, see section "Internet Group Management Protocol (IGMP) Status" in appendix B, "Monitoring and Analyzing Switch Operation" of the *Management and Configuration Guide* for your switch.

**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>Querier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>22</td>
<td>VLAN-2</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>33</td>
<td>VLAN-3</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

You could use the CLI to display this data as follows:
Example 2 Listing of IGMP configuration for all VLANs in the switch

HP Switch(config)# show ip igmp config

IGMP Service Config

Control unknown multicast [Yes] : Yes
Forced fast leave timeout [0] : 4
Delayed flush timeout [0] : 0

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>IGMP Enabled</th>
<th>Querier Allowed</th>
<th>Querier Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>Yes</td>
<td>No</td>
<td>125</td>
</tr>
<tr>
<td>22</td>
<td>VLAN-2</td>
<td>Yes</td>
<td>Yes</td>
<td>125</td>
</tr>
<tr>
<td>33</td>
<td>VLAN-3</td>
<td>No</td>
<td>Yes</td>
<td>125</td>
</tr>
</tbody>
</table>

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:

Figure 1 Listing of IGMP configuration for a specific VLAN

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>IGMP Enabled</th>
<th>Forward with High Priority</th>
<th>Querier Allowed</th>
<th>Querier Interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>VLAN-2</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>125</td>
</tr>
</tbody>
</table>

Port Type     | IP Mcast
--- ---------+ --------
B14 1000T    | Auto
B15 1000T    | Forward
B16 1000T    | Blocked

Viewing IGMP high level statistics for all VLANs on the switch

Syntax:

`show ip igmp statistics`
Example

Example 3 Displaying statistics for IGMP joined groups

HP Switch(config)# show ip igmp statistics

IGMP Service Statistics

Total VLAN's with IGMP enabled:  33
Current count of multicast groups joined:  21

IGMP Joined Group Statistics

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VLAN Name</th>
<th>Total</th>
<th>Filtered</th>
<th>Standard</th>
<th>Static</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DEFAULT_VLAN</td>
<td>52</td>
<td>50</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>22</td>
<td>VLAN-2</td>
<td>80</td>
<td>75</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>33</td>
<td>VLAN-3</td>
<td>1100</td>
<td>1000</td>
<td>99</td>
<td>1</td>
</tr>
</tbody>
</table>

Viewing IGMP historical counters for a VLAN

Syntax:

```
show ip igmp vlan vid counters
```

Example

Example 4 Display of IGMP historical counters for a VLAN

HP Switch(config)# show ip igmp vlan 1 counters

IGMP service Vlan counters

VLAN ID :  1
VLAN Name : DEFAULT_VLAN

General Query Rx :  58
General Query Tx :  58
Group Specific Query Rx : 3
Group Specific Query Tx : 3
V1 Member Report Rx : 0
V2 Member Report Rx : 2
V3 Member Report Rx : 0
Leave Rx : 0
Unknown IGMP Type Rx : 0
Unknown Pkt Rx : 0
Forward to Routers Tx Counter : 0
Forward to Vlan Tx Counter : 0
Port Fast Leave Counter : 0
Port Forced Fast Leave Counter : 0
Port Membership Timeout Counter : 0

Viewing IGMP group address information

Syntax:

```
show ip igmp groups
```
Example

Example 5 Displaying IGMP groups address information

```
HP Switch(vlan-2)# show ip igmp groups

IGMP Group Address Information

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Group Address</th>
<th>Expires</th>
<th>UpTime</th>
<th>Last Reporter</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>239.20.255.7</td>
<td>1h 2m 5s</td>
<td>1h 14m 5s</td>
<td>192.168.0.2</td>
<td>Filter</td>
</tr>
<tr>
<td>22</td>
<td>239.20.255.8</td>
<td>1h 2m 5s</td>
<td>1h 14m 5s</td>
<td>192.168.0.2</td>
<td>Standard</td>
</tr>
<tr>
<td>22</td>
<td>239.20.255.9</td>
<td>1h 2m 5s</td>
<td>1h 14m 5s</td>
<td>192.168.0.2</td>
<td>Static</td>
</tr>
</tbody>
</table>
```

Viewing IGMP group information for a VLAN with a filtered address

**Syntax:**
```
show ip igmp vlan vid group ip-addr
```

Example

Example 6 Group information for a VLAN with a filtered address group

```
HP Switch(config)# show ip igmp vlan 22 group 239.20.255.7

IGMP Service Protocol Group Info

VLAN ID: 22
VLAN NAME: VLAN-2

Filtered Group Address: 239.20.255.7
Last Reporter: 192.168.0.2
Up Time: 1 hr 14 min 5 sec

+-----------------+----------+--------+-------|
<table>
<thead>
<tr>
<th>Port</th>
<th>Port Type</th>
<th>Port Mode</th>
<th>Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>100/1000T</td>
<td>Auto</td>
<td>1 hr 2 min 5 sec</td>
</tr>
</tbody>
</table>
```

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. This command must be executed in a VLAN context.
Example

Example 7 Enable IGMP on VLAN 1

HP Switch(vlan-1)# vlan 1 ip igmp
Or
ip igmp

Example 8 Disable IGMP on VLAN 1

HP Switch(config)# no vlan 1 ip igmp

NOTE: 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 information on how switch memory operates, see chapter "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 traffic filters

Syntax:

    vlan vid ip igmp[ auto port-list | blocked port-list | forward port-list ]

Used in the VLAN context, specifies how each port should handle IGMP traffic. Default: auto.

NOTE: Where a static multicast filter is configured on a port, and an IGMP filter created by this command applies to the same port, the IGMP filter overrides the static multicast filter for any inbound multicast traffic carrying the same multicast address as is configured in the static filter. See section "Filter Types and Operation" in the "Port Traffic Controls" chapter of the Management and Configuration Guide for your switch.

Example

Suppose you want to configure IGMP as follows for VLAN 1 on the 100/1000T ports on a module in slot 1:

<table>
<thead>
<tr>
<th>Ports A1-A2</th>
<th>auto</th>
<th>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.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports A3-A4</td>
<td>forward</td>
<td>Forward all multicast traffic through this port.</td>
</tr>
<tr>
<td>Ports A5-A6</td>
<td>blocked</td>
<td>Drop all multicast traffic received from devices on these ports.</td>
</tr>
</tbody>
</table>
For a description of the default behavior of data-driven switches, see “Automatic fast-leave IGMP” (page 29).

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

HP Switch(config)# vlan 1 ip igmp auto a1,a2 forward a3,a4 blocked a5,a6
HP Switch(vlan-1)# 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.

HP Switch show igmp vlan 1 config

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.

The no version of the command disables the querier function on the switch. The show ip igmp config command displays the current querier command.

Default querier capability: Enabled

Configuring the querier interval

To specify the number of seconds between membership queries, enter this command with the desired interval.

Syntax:

[no] ip igmp querier interval [5-300]

NOTE: This command must be issued in a VLAN context.

Specifies the number of seconds between membership queries. The no form of the command sets the interval to the default of 125 seconds.

Default: 125 seconds

For example, to set the querier interval to 300 seconds on ports in VLAN 8:

HP Switch(vlan-8)# ip igmp querier interval 300

Configuring static multicast groups

Use this command to configure a group on the switch so that multicast traffic for that group can be forwarded with a receiver host. Traffic will be flooded for this group.

Syntax:

[no] ip igmp static-group group-address

NOTE: This command must be issued in a VLAN context.

Creates the IGMP static group with the specified group address on the selected VLAN. The no form of the command deletes the static group on the selected VLAN.
Configuring fast-leave IGMP

For information about fast-leave IGMP, see “Automatic fast-leave IGMP” (page 29).

Syntax:

```
[no] ip igmp fastleave port-list
```

- Enables IGMP fast-leaves on the specified ports in the selected VLAN.
- The `no` form of the command disables IGMP fast-leave on the specified ports in the selected VLAN.
- Use `show running` to display the ports per-VLAN on which fast-leave is disabled.
- Default: Enabled

Configuring forced fast-leave IGMP

For information about forced fast-leave, see “Forced fast-leave IGMP” (page 31).

Syntax:

```
[no] vlan vid ip igmp forcedfastleave port-list
```

- Enables IGMP forced fast-leave on the specified ports in the selected VLAN, even if they are cascaded.
- The `no` form of the command disables forced fast-leave on the specified ports in the selected VLAN.
- Use `show running` to display the ports per-VLAN on which forced fast-leave is enabled.
- Default: Disabled
- `show running-config` displays a non-default IGMP forced fast-leave configuration on a VLAN. The `show running-config` output does not include forced fast-leave if it is set to the default of 0.
- `forcedfastleave` can be used when there are multiple devices attached to a port.

Configuring fast learn

The fast learn option allows fast convergence of multicast traffic after a topology change. This command is executed in the global config context.

Syntax:

```
[no] igmp fastlearn port-list
```

- This command enabled fast learn on the specified ports. The `no` form of the command disables the fast learn function on the specified ports.
- Default: Disabled

Example 9 To enable fastlearn on ports 5 and 6

```
HP Switch(config)# igmp fastlearn 5-6
```

Configuring delayed group flush

When enabled, this feature continues to filter IGMP groups for a specified additional period of time after IGMP leaves have been sent. The delay in flushing the group filter prevents unregistered traffic from being forwarded by the server during the delay period. In practice, this is rarely
necessary on the switches, which support data-driven IGMP. (Data-driven IGMP, which is enabled by default, prunes off any unregistered IGMP streams detected on the switch.)

**Syntax:**

```plaintext
igmp delayed-flush time-period
```

Where leaves have been sent for IGMP groups, enables the switch to continue to flush the groups for a specified period of time. This command is applied globally to all IGMP-configured VLANs on the switch.

Range: 0 - 255; Default: Disabled (0)

**Syntax:**

```plaintext
show igmp delayed-flush
```

Displays the current `igmp delayed-flush` setting.

### Preventing unjoined multicast traffic

For more information about unjoined multicast traffic, see “Unjoined multicast traffic” (page 31).

**Syntax:**

```plaintext
[no] igmp filter-unknown-mcast
```

Enables interface isolation for unjoined multicast groups. IGMP is configured so that each interface with IGMP enabled will have a data-driven multicast filter associated with it, preventing unjoined IP multicast packets from being flooded. A reboot is required for the change to take effect.

Default: Disabled

### Configuring IGMP proxy (CLI)

For more information on IGMP proxy, see “IGMP general operation and features” (page 26).

### Adding or leaving a multicast domain

**Syntax:**

```plaintext
[no] igmp-proxy-domain domain-name[ border-router-ip-address | mcast-range | all ]
```

The no form of the command is used to remove a multicast domain.

All VLANs associated with the domain must first be removed for this command to work. See the no form of igmp-proxy in the VLAN context command.

- **domain-name**
  - User-defined name to associate with the PIM border router and multicast range that is being sent toward the border router.

- **border-router-ip-addr**
  - The IP address of the border router toward which IGMP proxy packets are sent. Not required for the no form of the command.

**NOTE:** The current routing FIB determines the best path toward the border router and therefore the VLAN that a proxy is sent out on

```plaintext
[ low-bound-ip-address | all ]
```

The low boundary (inclusive) of the multicast address range to associate with this domain (for example, 234.0.0.1).
If all is selected, the multicast addresses in the range of 224.0.1.0 to 239.255.255.255 are included in this domain.

**NOTE:** Addresses 224.0.0.0 to 224.0.0.255 are never used, because these addresses are reserved for protocols.

**high-bound-ip-address**
The high boundary (inclusive) of the multicast address range to associate with this domain (for example, 236.1.1.1).

**Examples**

**Example 10 IGMP proxy border IP address command**

This example shows the IGMP proxy border IP addresses (111.11.111.111) being configured.

```
HP Switch(config)# igmp-proxy-domain Bob 111.11.111.111
```

**Example 11 Setting the lower and upper bounds for multicasting**

This example shows the lower and upper boundaries of the multicast address range associated with the domain named Bob.

```
HP Switch(config)# igmp-proxy-domain Bob 111.11.111.111 234.0.0.1
HP Switch(config)# igmp-proxy-domain Bob 111.11.111.111 236.1.1.1
```

**Informs the VLAN which IGMP proxy domains to use with joins on the VLAN**

This command is performed when in VLAN context mode. When a query occurs on the upstream interface, an IGMP join is sent for all multicast addresses that are currently joined on the downstream interface.

**Syntax:**

```
[no] igmp-proxy domain-name
```

The no version of the command with no domain name specified removes all domains associated with this VLAN.

**NOTE:** Multiple different domains may be configured in the same VLAN context where the VLAN is considered the downstream interface. The domain name must exist prior to using this command to add the domain.

**NOTE:** If the unicast routing path to the specified IP address was through the specified VLAN, no proxy IGMP would occur, that is, a proxy is not sent back out on the VLAN that the IGMP join came in on.

If no unicast route exists to the border router, no proxy IGMP packets are sent.

**Viewing the IGMP proxy data**

**Syntax:**

```
show igmp-proxy [ entries | domains | vlans ]
```

Shows the currently active IGMP proxy entries, domains, or VLANs.
Examples

Example 12 Showing active IGMP proxy entries

HP Switch(config)# show igmp-proxy entries

Total number of multicast routes: 2

<table>
<thead>
<tr>
<th>Multicast Address</th>
<th>Border Address</th>
<th>VID</th>
<th>Multicast Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>234.43.209.12</td>
<td>192.168.1.1</td>
<td>1</td>
<td>George</td>
</tr>
<tr>
<td>235.22.22.12</td>
<td>15.43.209.1</td>
<td>1</td>
<td>SAM</td>
</tr>
<tr>
<td>226.44.3.3</td>
<td>192.168.1.1</td>
<td>2</td>
<td>George</td>
</tr>
</tbody>
</table>

Example 13 Showing IGMP proxy domains

HP Switch(config)# show igmp-proxy domains

Total number of multicast domains: 5

<table>
<thead>
<tr>
<th>Multicast Domain</th>
<th>Multicast Range</th>
<th>Border Address</th>
<th>Active entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>George</td>
<td>225.1.1.1/234.43.209.12</td>
<td>192.168.1.1</td>
<td>2</td>
</tr>
<tr>
<td>SAM</td>
<td>235.0.0.0/239.1.1.1</td>
<td>15.43.209.1</td>
<td>1</td>
</tr>
<tr>
<td>Jane</td>
<td>236.234.1.1/236.235.1.1</td>
<td>192.160.1.2</td>
<td>0</td>
</tr>
<tr>
<td>Bill</td>
<td>ALL</td>
<td>15.43.209.1</td>
<td>0</td>
</tr>
</tbody>
</table>

Example 14 Showing active IGMP proxy VLANs

HP Switch(config)# show igmp-proxy vlans

IGMP PROXY VLANs

<table>
<thead>
<tr>
<th>VID</th>
<th>Multicast Domain</th>
<th>Active entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>George</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>Sam</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>Jane</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>George</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>George</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>Bill</td>
<td>0</td>
</tr>
</tbody>
</table>

IGMP general operation and features

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. 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 is configured on the hosts, and multicast traffic is 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 used to manage IP multicast traffic through the switch. If no other querier is detected, the switch then also functions as the querier. If you need to disable the querier feature, do so through the IGMP configuration MIB, see “Configuring the querier function” (page 22).

**NOTE:** IGMP configuration on the switches operates at the VLAN context level. If you are not using VLANs, configure IGMP in VLAN 1 (the default VLAN) context.

---

**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**
      - (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.
    - **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” (page 28).

- **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 “About using the switch as querier” (page 36).

**NOTE:** 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 “Well-known or reserved multicast addresses excluded from IP multicast filtering” (page 37).

For more information about IGMP, see “How IGMP operates” (page 27).

---

**Number of IP multicast addresses allowed**

The number of IGMP filters (addresses) and static multicast filters available is 2,038. Additionally, 16 static multicast filters are allowed. If multiple VLANs are configured, then each filter is counted once per VLAN in which it is used.

**How IGMP operates**

IGMP is an internal protocol of the IP suite. IP manages multicast traffic by using switches, multicast routers, and hosts that support IGMP. A multicastrouter 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 sources is called 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, the switch must assume this function to elicit group membership information from the hosts on the network. If you need to disable the querier feature, do so through the CLI using the IGMP configuration MIB, see “Configuring the querier function” (page 22).

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 that 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 becomes 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 ceases 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.

To display IGMP data showing active group addresses, reports, queries, querier access port, and active group address data (port, type, and access), see section “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 “Comparison of IGMP operation with and without IP addressing” (page 29).
### Table 2 Comparison of IGMP operation with and without IP addressing

<table>
<thead>
<tr>
<th>IGMP function 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>
</tr>
<tr>
<td>Forward join requests (reports) to the Querier.</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Configure individual ports in the VLAN to Auto (the default)/Blocked, or Forward.</td>
<td>Yes</td>
<td>None</td>
</tr>
<tr>
<td>Configure IGMP traffic forwarding to normal or high-priority forwarding.</td>
<td>Yes</td>
<td>None</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>
</tr>
<tr>
<td>Support Fast-Leave IGMP and Forced Fast-Leave IGMP (below).</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Support automatic Querier election.</td>
<td>No</td>
<td>Querier operation not available.</td>
</tr>
<tr>
<td>Operate as the Querier.</td>
<td>No</td>
<td>Querier operation not available.</td>
</tr>
<tr>
<td>Available as a backup Querier.</td>
<td>No</td>
<td>Querier operation not available.</td>
</tr>
</tbody>
</table>

### Automatic fast-leave IGMP

Depending on the switch model, fast-leave is enabled or disabled in the default configuration.

<table>
<thead>
<tr>
<th>Switch model or series</th>
<th>Data-driven IGMP included?</th>
<th>IGMP fast-leave setting</th>
<th>Default IGMP behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch 8200zl Switch 6600 Switch 6400cl Switch 6200yl Switch 5400zl Switch 5300xl Switch 4200vl Switch 3500 Switch 3500yl Switch 3400cl Switch 2910 Switch 2900 Switch 2610 Switch 2510 Switch 2500</td>
<td>Yes</td>
<td>Always Enabled</td>
<td>Drops unjoined multicast traffic except for always-forwarded traffic toward the Querier or multicast routers and out of IGMP-forward ports. Selectively forwards joined multicast traffic, except on IGMP-forward ports, which forward all multicast traffic.</td>
</tr>
<tr>
<td>Switch 2600 Switch 2600-PWR Switch 4100gl Switch 6108</td>
<td>No</td>
<td>Disabled in the default configuration</td>
<td>IGMP fast-leave disabled in the default configuration. Floods unjoined multicast traffic to all ports. Selectively forwards joined multicast traffic, except on IGMP-forward ports, which forward all multicast traffic.</td>
</tr>
</tbody>
</table>
On switches that do not support data-driven IGMP, unregistered multicast groups are flooded to the VLAN rather than pruned. In this scenario, fast-leave IGMP can actually increase the problem of multicast flooding by removing the IGMP group filter before the Querier has recognized the IGMP leave. The Querier will continue to transmit the multicast group during this short time, and because the group is no longer registered, the switch will then flood the multicast group to all ports.

On HP switches that do support data-driven IGMP ("Smart" IGMP), when unregistered multicasts are received the switch automatically filters (drops) them. Thus, the sooner the IGMP leave is processed, the sooner this multicast traffic stops flowing.

Because of the multicast flooding problem mentioned above, the IGMP fast-leave feature is disabled by default on all HP switches that do not support data-driven IGMP (see the table above). The feature can be enabled on these switches via an SNMP set of this object:

\[\text{hpSwitchIgmpPortForceLeaveState.vid.port number}\]

However, HP does not recommend this, because it will increase the amount of multicast flooding during the period between the client's IGMP leave and the Querier's processing of that leave. For more information on this topic, see "Forced fast-leave IGMP" (page 31).

If a switch port has the following characteristics, the fast-leave operation will apply:

- Connected to only one end node.
- The end node currently belongs to a multicast group, that is, is an IGMP client.
- 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 Figure 2 (page 30), 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 2 Example of automatic fast-leave IGMP criteria**

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 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.

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 2 (page 30) belong to different VLANs, fast-leave does not operate on port A6.

**Default (enabled) IGMP operation solves the "delayed leave" problem**

Fast-leave IGMP is enabled by default. When fast-leave is disabled and 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 switch automatically 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.

Forced fast-leave IGMP

When enabled, 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 2 (page 30), 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.

Fast learn

The fast learn option allows fast convergence of multicast traffic after a topology change. This command is executed in the global config context.

Example 15 To enable fastlearn on ports 5 and 6

HP Switch(config)# igmp fastlearn 5-6

Unjoined multicast traffic

This feature adds a global IGMP multicast configuration option to the switch that results in each VLAN having a multicast filter. The filter prevents unjoined multicast traffic from being forwarded on interfaces associated with IGMP queriers. Each filter only contains interfaces that are queriers on the same VLAN, so multicast traffic is only flooded on interfaces that contain queriers that are on the same VLAN as the multicast traffic.

On switch bootup, all VLANs that are IGMP-enabled are guaranteed one multicast filter. You can always reboot the switch to recreate this configuration where each IGMP-enabled VLAN has a multicast filter.

NOTE: Joined multicast traffic continues to be forwarded as usual.

You must reboot the switch after configuring the per-VLAN filter.

Example 16 Enabling the IGMP multicast filter

HP Switch(config)# igmp filter-unknown-mcast
Command will take effect after saving configuration and reboot.

The following example shows the multicast traffic being flooded to all queriers on all VLANs; this is the default behavior. The igmp filter-unknown-mcast command has not been executed.

Table 3 Multicast filter table on distribution switch

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Member Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (all VLANs)</td>
<td>1, 2, 3</td>
</tr>
</tbody>
</table>
Figure 3 Example of unknown multicast traffic flooding on all ports connected to a querier for any VLAN

In the following example, igmp filter-unknown-mcast has been configured. The multicast traffic only goes to the querier on the same VLAN as the multicast server.

Table 4 Multicast filter table on distribution switch

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Member Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>1</td>
</tr>
<tr>
<td>200</td>
<td>2</td>
</tr>
<tr>
<td>300</td>
<td>3</td>
</tr>
</tbody>
</table>
To display the status of IGMP multicast filtering use the `show ip igmp` command. If the IGMP Filter Unknown Multicast setting is different from the IGMP Filter Unknown Multicast status, a reboot is required to activate the desired setting. This setting will then be reflected in the status.

**Example 17 IGMP unknown multicast filter setting being enabled but not yet activated**

```
HP Switch(config)# show igmp filter-unknown-mcast
IGMP Filter Unknown Multicast: Enabled
IGMP Filter Unknown Multicast Status: Disabled
```

To display information about IGMP multicast filtering by interface, use the `show ip igmp` command.

**IGMP proxy forwarding**

When a network has a border router connecting a PIM-SM domain to a PIM-DM domain, the routers that are completely within the PIM-DM domain have no way to discover multicast flows in the PIM-SM domain. When an IGMP join occurs on a router entirely within the PIM-DM domain for a flow that originates within the PIM-SM domain, it is never forwarded to the PIM-SM domain.

The IGMP proxy is a way to propagate IGMP joins across router boundaries. The proxy triggers the boundary router connected to a PIM-SM domain to query for multicast flows and forward them to the PIM-DM domain. IGMP needs to be configured on all VLAN interfaces on which the proxy is to be forwarded or received, and PIM-DM must be running for the traffic to be forwarded.

**NOTE:** For more information about PIM-DM and PIM-SM, see “PIM-DM (Dense Mode)” (page 38) and “PIM-SM (Sparse Mode)” (page 68).

You can configure an IGMP proxy on a selected VLAN that will forward IP joins (reports) and IGMP leaves to the upstream border router between the two multicast domains. You must specify the VLANs on which the proxy is enabled as well as the address of the border router to which the joins are forwarded.
How IGMP proxy forwarding works

The following steps illustrate how to flood a flow from the PIM-SM domain into the PIM-DM domain when an IGMP join for that flow occurs in the PIM-DM domain. See figure “IGMP proxy example” (page 34).

1. Configure Routing Switch 1 with the IGMP proxy forwarding function to forward joins toward Border Router 1; in addition, configure Routing Switch 1 to forward joins from VLAN 1 toward Border Router 2, as is VLAN 4 on Routing Switch 3.
2. Configure VLAN 2 on Routing Switch 2 to forward joins toward Border Router 1.
3. When the host connected in VLAN 1 issues an IGMP join for multicast address 235.1.1.1, the join is proxied by Routing Switch 1 onto VLAN 2 and onto VLAN 4. The routing information table in Routing Switch 1 indicates that the packet to Border Router 1 and Border Router 2 is on VLAN 2 and VLAN 4, respectively.

   **Figure 5 IGMP proxy example**

4. Routing Switch 2 then proxies the IGMP join into VLAN 3, which is connected to Border Router 1.
5. Border Router 1 uses PIM-SM to find and connect to the multicast traffic for the requested traffic. The traffic is flooded into the PIM-DM network where it is routed to the original joining host.
6. Additionally, the join was proxied from Routing Switch 3 to Border Router 2. At first, both border routers will flood the traffic into the PIM-DM domain. However, PIM-DM only forwards multicasts based on the shortest reverse path back to the source of the traffic as determined by the unicast routing tables (routing FIB). Only one multicast stream is sent to the joining host. This configuration provides a redundant in case the first fails.

Operating notes for IGMP proxy forwarding

- You can configure up to 12 multicast domains, which indicate a range of multicast addresses and the IP address of the PIM-SM/PIM-DM border router.
- You must give each domain a unique name, up to 20 characters.
• The domains may have overlapping multicast ranges.
• The IP address of the border router may be the same or different in each configured domain.
• Duplicate IGMP joins are automatically prevented, or leaves that would remove a flow currently joined by multiple hosts.
• Range overlap allows for redundant connectivity and the ability for multicasts to arrive from different border routers based on the shortest path back to the source of the traffic.
• The configured domain names must be associated with one or more VLANs for which the proxy joins are to be done.
• All routers in the path between the edge router receiving the initial IGMP packets and the border router have to be configured to forward IGMP using IGMP proxy.
• All upstream and downstream interfaces using IGMP proxy forwarding require IGMP and PIM to be enabled.
• You must remove all VLAN associations with the domain name before that domain name can be removed.
• The appropriate border routers must be used for each VLAN, or PIM-DM will not forward the traffic. This could occur when multiple border routers exist. It may be necessary to configure multiple overlapping domains if the multicast source address can generate the same multicast address and have different best paths to the PIM-DM domain.

⚠️ **CAUTION:** Be careful to avoid configuring a IGMP forward loop, because this would leave the VLANs in a joined state forever once an initial join is sent from a host. For example, a join is issued from the host in VLAN 2 and Routing Switch 2 will proxy the join onto VLAN 1. Routing Switch 3 will then proxy the join back onto VLAN 2 and increment its internal count of the number of joins on VLAN 2. Even after the host on VLAN 2 issues a leave, the proxy join will continue to remain and refresh itself each time a query occurs on VLAN 2. This type of loop could be created with multiple routers if an IGMP proxy is allowed to get back to the VLAN of the router that initially received the IGMP join from a host; see Figure 6 (page 36).
About 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 01/15/12 09:01:13 igmp: DEFAULT_VLAN: Other Querier detected
I 01/15/12 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, 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 01/15/12 09:21:55 igmp: DEFAULT_VLAN: Querier Election in process
I 01/15/12 09:22:00 igmp: DEFAULT_VLAN: This switch has been elected as Querier
```
Well-known or reserved multicast addresses excluded 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 predefined 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).

Table 5 (page 37) lists the 32 well-known address groups (8192 total addresses) that IGMP does not filter on.

### Table 5 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>

1. X is any value from 0 to 255.

**NOTE:** This operation applies to the HP Series 5400zl switches, the Series 3500yl switches, the switch 6200yl, the switch 8212zl, the Series 5300xl switches, as well as the 1600M, 2400M, 2424M, 4000M, and 8000M, but not to the Series 2500, 2650, Series 4100gl, Series 4200vl, 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-7fffff). 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 addresses 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.
## 2 PIM-DM (Dense Mode)

### Table 6 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] ip multicast-routing</td>
<td>Enables or disables IP multicast routing on the routing switch.</td>
<td>disabled</td>
<td>(page 40)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router pim</td>
<td>Enables or disables PIM at the global level and places the CLI in the PIM context.</td>
<td>disabled</td>
<td>(page 40)</td>
<td>-</td>
</tr>
<tr>
<td>router pim state-refresh 10 - 300</td>
<td>Sets the interval in seconds between successive state-refresh messages originated by the routing switch.</td>
<td>60 seconds</td>
<td>(page 40)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router pim trap [ all</td>
<td>neighbor-loss</td>
<td>hardware-mrt-full</td>
<td>software-mrt-full ]</td>
<td>Executed in the PIM context, enables and disables PIM SNMP traps.</td>
</tr>
<tr>
<td>[no] ip pim-dense [no] vlan vid ip pim</td>
<td>Enables multicast routing on the VLAN interface to which the CLI is currently set.</td>
<td>disabled</td>
<td>(page 42)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip pim-dense [ip-addr any</td>
<td>source-ip-address ]</td>
<td>Specifies the IP address to use as the source address for PIM protocol packets outbound on the VLAN.</td>
<td>primary VLAN</td>
<td>(page 43)</td>
</tr>
<tr>
<td>ip pim-dense [hello-interval 5-30 ] vlan vid ip pim-dense [hello-interval 5-30]</td>
<td>Changes the frequency at which the routing switch transmits PIM hello messages on the current VLAN</td>
<td>-</td>
<td>(page 43)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-dense [hello-delay 0-5] vlan vid ip pim-dense [hello-delay 0-5]</td>
<td>Changes the maximum time in seconds before the routing switch actually transmits the initial PIM hello message on the current VLAN.</td>
<td>5 seconds</td>
<td>(page 44)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-dense [graft-retry-interval 1-10] vlan vid ip pim-dense [graft-retry-interval 1-10]</td>
<td>Changing the interval the routing switch waits for the graft ack (acknowledgement) from another router before resending the graft request.</td>
<td>3 seconds</td>
<td>(page 44)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-dense [max-graft-retries 1-10] vlan vid ip pim-dense [max-graft-retries 1-10]</td>
<td>Changes the number of times the routing switch retries sending the same graft packet to join a flow.</td>
<td>3 attempts</td>
<td>(page 44)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-dense [lan-prune-delay] vlan vid ip pim-dense [lan-prune-delay]</td>
<td>Enables the LAN prune delay option on the current VLAN.</td>
<td>enabled</td>
<td>(page 45)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-dense [propagation-delay 250-2000]</td>
<td>Computes the lan-prune-delay</td>
<td>Propagation delay = 500</td>
<td>(page 45)</td>
<td>-</td>
</tr>
</tbody>
</table>
## Table 6 Summary of commands (continued)

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan vid ip pim-dense [propagation-delay 250-2000] ip pim-dense [override-interval 500-6000] vlan vid ip pim-dense [override-interval 500-6000]</td>
<td>setting for how long to wait for a PIM-DM join after receiving a prune packet from downstream for a particular multicast group.</td>
<td>milliseconds; override-interval = 2500 milliseconds</td>
<td>(page 46)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-dense [ttl-threshold 0-255] vlan vid ip pim-dense [ttl-threshold 0-255]</td>
<td>Sets the multicast datagram time-to-live (router hop-count) threshold for the VLAN.</td>
<td>0</td>
<td>(page 46)</td>
<td>-</td>
</tr>
<tr>
<td>show ip mroute</td>
<td>Lists VLANs actively forwarding routed, multicast traffic.</td>
<td>-</td>
<td>(page 48)</td>
<td>-</td>
</tr>
<tr>
<td>show ip mroute [interface vid]</td>
<td>Lists VLAN, protocol identity, and TTL settings</td>
<td>-</td>
<td>(page 49)</td>
<td>-</td>
</tr>
<tr>
<td>show ip mroute [multicast-ip-addr source-ip-addr]</td>
<td>Lists data for the specified flow (multicast group).</td>
<td>-</td>
<td>(page 50)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim</td>
<td>Displays PIM status and global parameters.</td>
<td>-</td>
<td>(page 52)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim [interface]</td>
<td>Lists the PIM interfaces (VLANs) currently configured in the routing switch.</td>
<td>-</td>
<td>(page 53)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim [interface [vid]]</td>
<td>Displays the current configuration for the specified VLAN (PIM interface)</td>
<td>-</td>
<td>(page 54)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim [mroute]</td>
<td>Shows PIM-specific information from the IP MRT</td>
<td>-</td>
<td>(page 55)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim [mroute [multicast-group-address multicast-source-address]]</td>
<td>Displays the PIM route entry information for the specified multicast group (flow).</td>
<td>-</td>
<td>(page 55)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim [neighbor]</td>
<td>Lists PIM neighbor information for all PIM neighbors connected to the routing switch.</td>
<td>-</td>
<td>(page 56)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim [neighbor [ip-address ]]</td>
<td>Lists the same information as show ip pim [neighbor] (page 56) for the specified PIM neighbor.</td>
<td>-</td>
<td>(page 56)</td>
<td>-</td>
</tr>
</tbody>
</table>

For introductory and general information, see the sections beginning with “About PIM-DM” (page 57).

### Overview

This chapter describes protocol-independent multicast (PIM) routing operation on the switches covered in this guide and how to configure it with the switch’s built-in interfaces. It is assumed that you have an understanding of multimedia traffic control with IP multicast (IGMP), see “Multimedia Traffic Control with IP Multicast (IGMP)” (page 15).
Global and PIM configuration contexts

**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.

Enabling or disabling IP multicast routing

Syntax:

```
[no] ip multicast-routing
```

Enables or disables IP multicast routing on the routing switch. IP routing must be enabled.

Default: Disabled

Enabling or disabling PIM at the global level; placing the CLI in the PIM context

Syntax:

```
[no] router pim
```

Enables or disables PIM at the global level and places the CLI in the PIM context. IP routing must first be enabled.

Default: Disabled.

Setting the interval in seconds between successive state-refresh messages originated by the routing switch

Syntax:

```
router pim state-refresh [10-300]
```

Executed in the PIM context, this command sets the interval in seconds between successive state-refresh messages originated by the routing switch. 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

Enabling and disabling PIM SNMP traps

Syntax:

```
[no]router pim trap[[all] | neighbor-loss | hardware-mrt-full | software-mrt-full ]
```

Executed in the PIM context, this command 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 hardwareMRT is full (2048 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 MRT is full (routing resources for active flows are exhausted.)
   Default: Disabled

**NOTE:** In this state, the routing switch does not accept any additional flows.
Example 18 Example of configuring PIM in the Global and PIM context

In Figure 11 (page 61), the "#1" routing switch is directly connected to the multicast sources for the network. For this example, suppose that you are choosing the following:

- Reduce the state-refresh time from the default 60 seconds to 30 seconds. (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 2048 active flows.

To configure global-level PIM operation for the "8212zI #1" routing switch, you would use the commands shown in Figure 7 (page 42).

Figure 7 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. See Table 7 (page 54).

PIM VLAN (interface) configuration context

Enabling multicast routing on the VLAN interface to which the CLI is currently set

Syntax:

```
[no]ip pim-dense
```
[no]vlanvidip 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

Specifying the IP address to use as the source address for PIM protocol packets outbound on the VLAN

Syntax:

[no]ip pim-dense [ ip-addr any | sourceip-address ]
[no]vlan [vid]ip pim-dense [ ip-addr | any | sourceip-address ]

In networks using multi-netted VLANs, all routers on a given VLAN intended to route multicast packets must have at least one common subnet on that VLAN. Use this command when the VLAN is configured with multiple IP addresses (multi-netting) 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 multi-netted VLAN are not configured with identical sets of subnet IP addresses.
- Use all if the multi-netted VLAN is configured with the same set of subnet addresses.

Default: the primary VLAN

Changing the frequency at which the routing switch transmits PIM hello messages on the current VLAN

Syntax:

ip pim-dense [ hello-interval 5-30 ]
vlan [vid]ip pim-dense [hello-interval 5-30]

Changes the frequency at which the routing switch transmit 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.

**NOTE:** Not used with the [no] form of the ip pim-dense command.
Example 19 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 that 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), the shorter hello interval causes it to stop transmitting multicast traffic onto the VLAN sooner, resulting in less unnecessary bandwidth usage.

Changing the maximum time in seconds before the routing switch actually transmits the initial PIM hello message on the current VLAN

Syntax:

```
ip pim-dense [hello-delay 0-5]
vlan [vid] ip pim-dense [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, 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.

**NOTE:** Not used with the [no] form of the ip pim-dense command.

Default: 5 seconds

Changing the interval the routing switch waits for the graft ack from another router before resending the graft request

Syntax:

```
ip pim-dense [graft-retry-interval[1-10]]
vlan [vid] ip pim-dense [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 (acknowledgement) is not received within the time period of the graft-retry-interval, it resends the graft packet. The command [graft-retry-interval[1-10]] changes the interval (in seconds) the routing switch waits for the graft ack from another router before resending the graft request.

**NOTE:** Not used with the [no] form of the ip pim-dense command.

Default: 3 seconds

Changing the number of times the routing switch retries sending the same graft packet to join a flow

Syntax:

```
ip pim-dense [max-graft-retries[1-10]]
vlan [vid] ip pim-dense [max-graft-retries[1-10]]
```
Changes to 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.

**NOTE:** Not used with the [no] form of the ip pim-dense command.

Default: 3 attempts

### Enabling the LAN prune delay option on the current VLAN

**Syntax:**

```
ip pim-dense [lan-prune-delay]
```

```
[lan-prune-delay]
```

Vlan

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 request to override the prune before the lan-prune-delay times out 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 determine the lan-prune-delay setting. See “Computing the lan-prune-delay setting” (page 45).

**NOTE:** Uses the [no] form of the ip pim-dense command to disable the LAN prune delay option.

Default: Enabled

### Computing the lan-prune-delay setting

**Syntax:**

```
ip pim-dense [propagation-delay[250-2000]]
```

```
[propagation-delay[250-2000]]
```

Vlan

```
ip pim-dense [override-interval[500-6000]]
```

```
[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 for how long to wait for a PIM-DM Join after receiving a prune packet from downstream for a particular multicast group.

Defaults: propagation-delay=500 milliseconds; override-interval = 2500 milliseconds
Example 20 Upstream router prune

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 prune 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. If no routers on the VLAN send a Join, the upstream router prunes group "X" from VLAN "Y" when the lan-prune-delay timer expires.

Setting the multicast datagram time-to-live (router hop-count) threshold for the VLAN

Syntax:

```
ip pim-dense [ttl-threshold[0-255]]
```

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

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.

The VLAN connected to the multicast source does not receive state refresh packets and thus is not state-refresh capable. Downstream VLANs in the switches covered in this guide are state-refresh capable. 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. 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 8 (page 47) uses VLAN 25 for multicast traffic. However, this VLAN is multinetted and there is only one subnet (10.38.10.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-dense 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, the `ip pim-dense ip-addr any` command would be used instead.) The other VLANs in the network are not multinetted and therefore do not require the `ip pim-dense ip-addr any` option.

For this example, assume that the VLANs and IP addressing are already configured on the routing switch.
Figure 8 Multicast network with a multinetted VLAN

On the three routing switches, VLAN 25 is multinetted with subnets that match in only one instance. Since subnet 10.38.10.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.)

---

HP Switch(config)# vlan 25
HP Switch(vlan-25)# ip igmp
HP Switch(vlan-25)# ip rip
HP Switch(vlan-25)# ip pim-dense ip-addr 10.38.10.1
HP Switch(vlan-25-pim-dense)# vlan 27
HP Switch(vlan-27)# ip igmp
HP Switch(vlan-27)# ip rip
HP Switch(vlan-27)# ip pim-dense
HP Switch(vlan-27-pim-dense)# vlan 29
HP Switch(vlan-29)# ip igmp
HP Switch(vlan-29)# ip rip
HP Switch(vlan-29)# ip pim-dense
HP Switch(vlan-29-pim-dense)# write mem
HP Switch(vlan-29-pim-dense)# exit
HP Switch(vlan-29)# exit

---

Figure 8 (page 47) illustrates the steps for configuring multicast routing at the VLAN level for the 8212zl switch #1 shown in Figure 8 (page 47).
Displaying PIM data and configuration settings

Displaying PIM route data

Syntax:

```
show ip [mroute]
```

Without parameters, lists multicast route entries in the following situations:

- When the PIM-DM router is actively forwarding a multicast flow out an interface (VLAN.)
- On a PIM-DM originator router (source directly connected) when traffic is entering the router but not forwarding

**NOTE:** The neighbor field will be empty in this case.

- On a PIM-DM Non-originator router for a short duration after a flow’s initial flood/prune cycle is seen. This entry is cleared after 5 minutes unless the flow is connected within that time period.

[Group Address]

The multicast group IP address for the specific flow (source-group pair.)
Source Address
The unicast address of the flow's source.

Neighbor
The IP address of the upstream multicast router interface (VLAN) from which the multicast flow is coming. A blank field indicates that the multicast source is directly connected to the router.

VLAN
The interface on which the router receives the multicast flow.

Example 21: Showing the route entry data on the “#2” routing switch

The next figure displays the `show ip mroute` output on the “8212zl #2” routing switch shown in Figure 8 (page 47). This case illustrates two multicast groups from the same multicast source.

```
HP Switch(config)# show ip mroute
IP Multicast Route Entries
Total number of entries : 2
Group Address Source Address Neighbor VLAN
-------------------------- --------------------- -----
239.255.255.1 10.27.30.2 10.29.30.1 29
239.255.255.5 10.27.30.2 10.29.30.1 29
```

Displays the PIM interfaces currently configured

**Syntax**

```
show ip mroute [interface vid]
```

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.

**Example 22: Output for routing switch “#1”**

```
HP Switch(config)# show ip mroute interface
PIM Interfaces
VLAN IP Address Mode
---- --------------- ------------
25 10.38.10.1 dense
27 10.27.30.1 dense
29 10.29.30.1 dense
```

Viewing VLAN, protocol identity, and TTL settings

**Syntax:**

```
show ip [mroute] [interface vid]
```
Example 23 The show ip mroute interface command on routing switch "#2" in Figure 8 (page 47)

<table>
<thead>
<tr>
<th>HP Switch(config)# show ip mroute interface 29</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Multicast Interface</td>
</tr>
<tr>
<td>VLAN     : 29</td>
</tr>
<tr>
<td>Protocol : PIM-DM</td>
</tr>
<tr>
<td>TTL Threshold : 0</td>
</tr>
</tbody>
</table>

Viewing data for a specified flow (multicast group)

Syntax:

```bash
show ip [mroute] [multicast-ip-addr source-ip-addr]
```

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

- **Group Address**
  - The multicast group IP address for the specified flow.
- **Source Address**
  - The source IP address for the specified flow.
- **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**
  - The interface on which the router receives the 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.

**NOTE:** On an originator router, when a forwarding flow moves to a non-forwarding state (i.e. when pruned) the Up Time value for that flow is reset to 0.

- **Expire Time (Sec)**
  - An mroute which is in a forwarding state — one which represents an active, connected flow for which there are downstream routers and/or locally connected hosts interested in the flow — does not expire. When other PIM-DM routers or locally connected hosts are no longer interested in an active flow, the related mroute on an originator router moves to a blocking state, and an mroute in this state does not expire either. In both cases the mroute is only removed by the system when it is no longer needed and so the displayed value for expire time in these situations is not meaningful.
  - For an mroute on an originator router whose flow is no longer active - including mroutes on non-originators whose flow has been pruned — expire time indicates when the mroute entry will eventually be cleared.

**Multicast Routing Protocol**

Identifies the multicast routing protocol through which the current flow was learned.
Unicast Routing Protocol
Identifies the IP routing protocol through which the routing switch learned the upstream interface for the current multicast flow. The listed protocol will be one of the following:

- RIP
- connected
- OSPF
- static route
- other

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.)

Asset Timer
The time remaining until the router 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 router assumes it is the best path, and the specified multicast group traffic will flow through the router.

RP Tree
This field is not relevant to PIM-DM and will always display No.

Downstream interfaces
For each downstream interface the following information is shown:

[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)
The natural state of a downstream interface in PIM-DM is to forward multicast flows and DM will flood a new flow out all interfaces on a router where there
are connected PIM-DM neighbors and/or joined hosts. If there are ultimately no receivers for the flow downstream, the flow will be pruned back to the originator router. This prune state is maintained on all PIM-DM routers by state refresh message sends by the originator and corresponding prune replies from downstream routers. However if a prune reply is not received (i.e. there is now a receiver), expire time indicates how long before the interface will return to a forwarding state.

**Expire Time (sec)**

The natural state of a downstream interface in PIM-DM is to forward multicast flows and DM will flood a new flow out all interfaces on a router where there are connected PIM-DM neighbors and/or joined hosts. If there are ultimately no receivers for the flow downstream, the flow will be pruned back to the originator router. This prune state is maintained on all PIM-DM routers by state refresh message sends by the originator and corresponding prune replies from downstream routers. However if a prune reply is not received (i.e. there is now a receiver), expire time indicates how long before the interface will return to a forwarding state.

**Example 24 Example output for routing switch "#1" in Figure 8 (page 47)**

A populated neighbor field indicates that the multicast server is directly connected to the routing switch (neighbor field is highlighted in bold below).

```
HP Switch(config)# show ip mroute 239.255.255.5 10.27.30.2
IP Multicast Route Entry
Group Address : 239.255.255.5
Source Address : 10.27.30.2
Source Mask : 255.255.255.0
Neighbor : 10.30.229.1
VLAN : 27
Up time (sec) : 408
Expire Time (sec) : 150
Multicast Routing Protocol : PIM-DM
Unicast Routing Protocol : rip

Downstream Interfaces
<table>
<thead>
<tr>
<th>VLAN</th>
<th>State</th>
<th>Up time (sec)</th>
<th>Expire Time (sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>pruned</td>
<td>408</td>
<td>98</td>
</tr>
</tbody>
</table>
```

**Displaying PIM status**

**Syntax:**

```
show ip pim [mroute]
```

This command displays exactly the same output as the command `show ip [mroute]`.

**Displaying PIM neighbor data**

**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.
- **Expire Time**: Indicates how long before the router will age-out a PIM neighbor/adjacency relationship on the specified interface (VLAN). When a neighbor/adjacency expires and that neighbor was the last one on the interface, multicast data and state refresh packets will no longer be sent out that interface. Receipt of a periodic PIM hello message from the neighboring PIM router resets this timer to the hold time value stored in the hello message. If the ip-addr is specified then detailed information for the specified neighbor is shown.

### Example 25 Example of PIM neighbor output

This example simulates output from routing switch “#1” in Figure 8 (page 47).
The data identifies the first downstream neighbor (“routing switch #2”).
HP Switch(config)# show ip pim neighbor
PIM Neighbors
IP Address VLAN Up Time (sec) Expire Time (sec)
----------------- ---- ------------------ ------------------
10.29.30.2 29 196 89

### Variation

**Syntax**

```
show ip pim [neighbor]
```

Lists the same information as `show ip pim neighbor` found on (LINK) for the specified PIM neighbor:

This example simulates output from routing switch “#1” in Figure 8 (page 47).
The data is from the first downstream neighbor (routing switch “#2”).
HP Switch(config)# show ip pim neighbor 10.29.30.2
PIM Neighbor
IP Address : 10.29.30.2
VLAN : 29
Up Time (sec) : 26
Expire Time (sec) : 79

### Listing the PIM interfaces (VLANs) currently configured in the routing switch

**Syntax:**

```
show ip pim [interface]
```

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

```
[VID]
```

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).
Shows dense only.

Example 26 Output for routing switch "#1" in Figure 8 (page 47)

```
HP Switch(config)# show ip pim interface
PIM Interfaces
  VLAN IP Address     Mode
    ---- --------------- ------------
      25          10.38.10.1  dense
      27          10.27.30.1  dense
      29          10.29.30.1  dense
```

Viewing the current configuration for the specified VLAN (PIM interface)

Syntax:

```
show ip pim [interface [vid]]
```

Displays the current configuration for the specified VLAN (PIM interface). See Table 7 (page 54).

Example 27 Example output for routing switch "#1" in Figure 8 (page 47)

```
HP Switch(config)# show ip pim interface 29
PIM Interface
  VLAN       : 29
  IP Address : 10.29.30.1
  Mode       : dense
  Hello Interval (sec) : 30
  Hello Delay (sec) : 5
  Graft Retry Interval (sec) : 3
  Max Graft Retries : 2
  Override Interval (msec) : 2500  Lan Prune Delay
    : Yes
  Propagation Delay (msec) : 500  Lan Delay Enabled
    : No
  SR TTL Threshold : 2  State Refresh Capable
    : No
```

Table 7 PIM interface configuration settings

<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><code>vlan vid ip pim-dense</code></td>
</tr>
<tr>
<td>IP</td>
<td>N/A</td>
<td>`vlan vid ip pim-dense any</td>
</tr>
<tr>
<td>Mode</td>
<td><code>dense</code></td>
<td>PIM-dense or PIM-sparse</td>
</tr>
<tr>
<td>Hello interval (sec)</td>
<td>30</td>
<td><code>ip pim-dense hello interval 5 - 30</code></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. See the description of the hello interval on (page 42).</td>
</tr>
<tr>
<td>Hello delay</td>
<td>5</td>
<td><code>vlan vid ip pim-dense hello delay 0 - 5</code></td>
</tr>
<tr>
<td>Graft retry interval (sec)</td>
<td>3</td>
<td><code>vlan vid ip pim-dense graft-retry-interval 1 - 10</code></td>
</tr>
<tr>
<td>Field</td>
<td>Default</td>
<td>Control command</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Max graft retries</td>
<td>2</td>
<td>vlan vid ip pim-dense graft-retries 1 - 10</td>
</tr>
<tr>
<td>Override interval (msec)</td>
<td>2500</td>
<td>vlan vid ip pim-dense override-interval 500 - 6000</td>
</tr>
<tr>
<td>Propagation delay (msec)</td>
<td>500</td>
<td>vlan vid ip pim-dense propagation-delay 250-2000</td>
</tr>
<tr>
<td>SR TTL threshold (router hops)</td>
<td>0</td>
<td>vlan vid ip pim-dense ttl-threshold 0 - 255</td>
</tr>
<tr>
<td>LAN prune delay</td>
<td>Yes</td>
<td>vlan vid ip pim-dense lan-prune-delay</td>
</tr>
<tr>
<td>LAN delay enabled</td>
<td>No</td>
<td>Showing [Yes] if all multicast routers on the current VLAN interface enabled LAN-prune-delay. Otherwise, shows [No]</td>
</tr>
<tr>
<td>State-refresh capable</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 the switches are state-refresh capable.</td>
</tr>
</tbody>
</table>

Viewing PIM-specific information from the IP multicast routing table (MRT)

Syntax:
```
show ip pim [mroute]
```
This command displays exactly the same output as the command `show ip [mroute]`.

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

Syntax:
```
show ip pim [mroute[multicast-group-address multicast-source-address]]
[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
   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, 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, 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).

Example 28 Example from routing switch "#1" in Figure 8 (page 47) showing a multicast group from a directly connected source

```
HP Switch(config)# show ip pim mroute 239.255.255.1 10.27.30.2
PIM Route Entry
   Group Address : 239.255.255.1
   Source Address : 10.27.30.2
   Source Mask : 255.255.255.0
   Metric :3
   Metric Pref :120
   Assert Timer : 0
Downstream Interfaces
   VLAN Prune Reason
   ---- ------------
   28   prune
```

Listing PIM neighbor information for all PIM neighbors connected to the routing switch

Syntax:
```
show ip pim [neighbor]
```

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.

Expire 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, detailed information for the specified neighbor is shown.

**Example 29 PIM neighbor output**

This example simulates output from routing switch “#1” in Figure 8 (page 47). The data identifies the first downstream neighbor (“routing switch #2”).

```
HP Switch(config)# show ip pim neighbor
PIM Neighbors
IP Address      VLAN Up Time (sec)      Expire Time (sec)
--------------- ---- ------------------ ------------------
10.29.30.2      29   196                89
```

**Syntax:**
```
show ip pim [neighbor [ ip-address ]]
```
Lists the same information as the `show ip pim neighbor`

**Example 30 Showing a specific neighbor**

This example simulates output from routing switch “#1” in Figure 8 (page 47). The data is from the first downstream neighbor (routing switch “#2”).

```
HP Switch(config)# show ip pim neighbor 10.29.30.2
PIM Neighbor
IP Address : 10.29.30.2
VLAN : 29
Up Time (sec) : 26
Expire Time (sec) : 79
```

**About PIM-DM**

In a network where IP multicast traffic is transmitted for multimedia applications, traffic is blocked at routed interface (VLAN) boundaries unless a multicast routing protocol is running. PIM is a family of routing protocols that form multicast trees to forward traffic from multicast sources to subnets are using a protocol such as IGMP to request the traffic. PIM relies on the unicast routing tables created by any of several unicast routing protocols to identify the path back to a multicast source, known as reverse path forwarding (RPF). Based on information provided by the unicast routing tables,
PIM sets up a distribution tree for the multicast traffic. The PIM-DM and PIM-SM protocols on the switches enable and control multicast traffic routing.

IGMP provides the multicast traffic link between a host and a multicast router running PIM-DM or PIM-SM. IGMP and either PIM-DM or PIM-SM must be enabled on VLANs whose member ports have directly connected hosts with a valid need to join multicast groups. 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.

License requirements:
In the 3500yl, 5400zl, and 6600 and 8200zl switches, PIM-DM is included with the Premium License. In the 6200yl switches, this feature is included with the base feature set.

PIM-DM features
PIM-DM features on switches covered by this guide include:

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

VLAN interface support
The MRT supports up to 128 outbound VLANs at any given time. The sum of all outbound VLANs across all current flows on a router may not exceed 128. (A single flow may span one inbound VLAN and up to 128 outbound VLANs, depending on the VLAN memberships of the hosts actively belonging to the flow.)

Flow capacity
Up to 2048 flows are supported in hardware across a maximum of 128 outbound VLANs. (A flow is composed of an IP source address and an IP multicast group address, regardless of the number of active hosts belonging to the multicast group at any given time.)

IGMP compatibility
PIM-DM is compatible with IGMP (V1 to V3) and is fully interoperable with IGMP for determining multicast flows.

VRRP
PIM-DM is fully interoperable with VRRP 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. See “Exceptions to Support for RFC 2932 - Multicast Routing MIB” (page 66).

PIM draft specifications
Compatible with PIM-DM draft specifications (V1 and V2).

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 which have 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. The flow destination is the multicast group address and not a specific host or VLAN. 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.

PIM-DM interoperates with IGMP and the switch’s routing protocols for the switches covered by this guide. The PIM operates independently of the routing protocol you choose to run on your switches. This means that you can use PIM-DM with RIP, OSPF, or static routes configured. PIM-DM uses 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 routing method is known as reverse path forwarding (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, see Figure 10 (page 59). 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.

**Figure 10 Example of multicast tree for a given flow**

When the routing switch detects a new multicast flow, it initially floods the traffic throughout the PIM-DM domain, then it prunes the traffic on the branches (network paths) where joins have not been received from individual hosts. This creates the tree structure shown in Figure 10 (page 59). 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. See “PIM VLAN (interface) configuration context” (page 42).

### Multicast flow management

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

#### Initial flood and prune

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. (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; this means that 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 multicast switch, if directly connected to a multicast source (such as a video conference application), periodically transmit 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, 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:** 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.

See Figure 11 (page 61) for an example of bandwidth conservation.
Figure 11 Bandwidth conservation in switches with PIM-DM state-refresh

General configuration elements

PM-DM requires you to configure the following elements:

- IP routing enabled on all routing switches you want to carry routed multicast traffic.
- Routing methods 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.
- Enable IP multicast routing.
- Enable IGMP on each VLAN when that VLAN has hosts that you want to join multicast groups. Repeat this action on every switch and router belonging to the VLAN.
- 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, it is recommended that you leave the PIM-DM configuration parameters at their default settings. From the default, you can assess performance and make configuration changes when needed.

About configuring PIM-DM

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:
   - 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: enable the same option on each VLAN where you want multicast routing to operate.
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

Operating notes

PIM-DM operating rules

- The routing switch supports 2048 multicast flows in hardware. See, “Flow capacity” (page 62).
- The multicast routing table (MRT) that PIM-DM creates allows up to 128 outbound VLANs at any given time. PIM-DM supports multicast routing across 128 VLANs.
- The routing switch allows one instance of PIM per VLAN. For networks using multinetted VLANs, all routers on the intended VLAN must have at least one common subnet if you intend on routing multicast packets. The routing switch provides a command for specifying which IP address PIM will use on each VLAN.

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 switches covered in this guide 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 downstream multicast routers are switches covered in this guide. (The HP 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 2048 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.)

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. See “Configuring the querier function” (page 22).

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 MRT to add another multicast group. Software will route any multicast packets sent to multicast groups that are not in the hardware MRT, but it will be slower, and packets may be dropped if the data rate is greater than 3000 packets per second. See “Flow capacity” (page 62).

NOTE: The PIM protocol uses one MRT entry for every IP multicast S/G 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.

Heavy memory usage

Heavy use of PIM (many S/G flows over many VLANs), combined with other memory-intensive features, can oversubscribe memory resources and impact overall performance. If available memory is exceeded, the switch drops any new multicast flows and generates appropriate Event Log messages. Corrective actions can include:

- Reducing the number of VLANs on the switches by moving some VLANs to another device.
- Freeing up system resources by disabling another, non-PIM feature.
- Moving some hosts to another device.

For more information, see “Operating notes” (page 62) and “Messages related to PIM operation” (page 63).

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. See "Using the Event Log To Identify Problem Sources" in the "Troubleshooting" appendix of the latest version of the Management and Configuration Guide for your switch. (The latest version of all HP switch documentation is available on the HP website at www.hp.com/manuals.)

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>alpha-string pkt, src IP ip-addr vid vlan-id (not a nbr) (counter)</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 source-ip-addr (counter)</td>
<td>The switch detected a TTL of 0 (zero) in the PIM portion of a state-refresh packet. (This is not the IP TTL)</td>
</tr>
<tr>
<td>Message</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Failed alloc of HW alpha-str for flow multicast-address, source-address (dup-msg-cnt)</td>
<td>There are more than 2048 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 data-type pkt (counter)</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. If the number of flows exceeds 2048, 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 text-str as a call back routine (counter)</td>
<td>Indicates an internal error. Report the incident to your HP customer care center and reinstall the router software.</td>
</tr>
<tr>
<td>I/F configured with IP ip-address on vid vlan-id (counter)</td>
<td>Indicates that the interface (VLAN) has been configured with the indicated IP address. At boot-up or when an IP address is changed, the switch generates this message for each PIM-configured VLAN.</td>
</tr>
<tr>
<td>I/F removal with IP ip-addr on vid vlan-id (counter)</td>
<td>Indicates that a PIM interface (VLAN) has been removed from the router as a result of an 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 because of one of the following causes:  
  • No PIM interface on the VLAN  
  • Bad packet length  
  • Bad IP header length  
  • Bad IP total length |
<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkt rcvd with a cksum error from ip-addr (counter)</td>
<td>A packet having a checksum error was received from ip-address. Check the cabling and ports on the local and the remote routers.</td>
</tr>
<tr>
<td>Rcvd incorrect hello from ip-addr (counter)</td>
<td>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.</td>
</tr>
<tr>
<td>Rcvd text-str pkt with bad len from ip-addr (counter)</td>
<td>A peer router may be sending incorrectly formatted PIM packets.</td>
</tr>
<tr>
<td>Rcvd hello from ip-address on vid vlan-id (counter)</td>
<td>Indicates a misconfiguration where two routers are directly connected with different subnets on the same connected interface.</td>
</tr>
<tr>
<td>Rcvd pkt from rtr ip-address , unkwn pkt type value (counter)</td>
<td>A packet received from the router at ip-address is an unknown PIM packet type. (The value variable is the numeric value received in the packet.)</td>
</tr>
<tr>
<td>Rcvd pkt ver# ver-num , from ip-address , expected ver-num (counter)</td>
<td>The versions of PIM-DM on the sending and receiving routers do not match. Differing versions are typically compatible, but features not supported in both versions will not be available.</td>
</tr>
<tr>
<td>Rcvd unkwn addr fmly addr-type in text-str pkt from ip-addr (counter)</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 opt-nbr in text-string pkt from ip-addr (counter)</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( failure-type ) on packet-type pkt on VID vid ( counter)</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 text-str table (counter)</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></td>
<td>- Reduce the number of configured VLANs by moving some VLANs to another router.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>- Move some hosts that create multicast demand to another router.</td>
</tr>
<tr>
<td>Unable to alloc a buf of size bytes for data-flow (counter)</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></td>
<td>- Reduce the number of configured VLANs by moving some VLANs to another router.</td>
</tr>
<tr>
<td></td>
<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>
</tr>
<tr>
<td></td>
<td>- Move some hosts that create multicast demand to another router.</td>
</tr>
<tr>
<td>Message</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</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 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, see "Exceptions to Support for RFC 2932 - Multicast Routing MIB".
- RFC 2933 - IGMP MIB
- RFC 2934 - Protocol Independent Multicast MIB for IPv4

### Exceptions to Support for RFC 2932 - Multicast Routing MIB

These MIB objects are not supported:

- ipMRouteInterfaceRateLimit
- ipMRouteInterfaceINMcastOctets
- ipMRouteInterfaceOUTMcastOctets
- ipMRouteInterfaceHCINMcastOctets
- ipMRouteInterfaceHCOOUTMcastOctets
- ipMRouteBoundaryTable
- ipMRouteBoundaryEntry
- ipMRouteBoundaryIfIndex
- ipMRouteBoundaryAddress
- ipMRouteBoundaryAddressMask
- ipMRouteBoundaryStatus OBJECT-TYPE
- ipMRouteScopeNameTable
- ipMRouteScopeNameEntry
- ipMRouteScopeNameAddress
- ipMRouteScopeNameAddressMask
- ipMRouteScopeNameLanguage
- ipMRouteScopeNameString
- ipMRouteScopeNameDefault
- ipMRouteScopeNameStatus
# 3 PIM-SM (Sparse Mode)

For introductory information, see “PIM-SM overview” (page 101).

## Table 8 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] ip routing</td>
<td>Enables IP routing on the router.</td>
<td>Disabled</td>
<td>(page 71)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip multicast-routing</td>
<td>Enables or disables IP multicast routing on the router.</td>
<td>Disabled</td>
<td>(page 71)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router [ ospf</td>
<td>rip ]</td>
<td>[no] ip route [ ip-addr/mask-len ] [ ip-addr</td>
<td>vlan</td>
<td>reject</td>
</tr>
<tr>
<td>[no] router pim</td>
<td>Enables PIM at the global level and puts the CLI into the PIM context level.</td>
<td>Disabled</td>
<td>(page 71)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-sparse [ ip-addr any</td>
<td>ip-addr ] vlan vid ip pim-sparse [ ip-addr any</td>
<td>ip-addr ] no[vlan vid]ip pim-sparse</td>
<td>Enables or disables PIM-SM in the designated VLAN interface and sets the source (and designated router) IP address for PIM-SM packets sent from the interface.</td>
<td>Disabled</td>
</tr>
<tr>
<td>ip pim-sparse hello-interval 5-300 vlan vid ip pim-sparse hello-interval 5-300</td>
<td>Changes the frequency at which the router transmits PIM hello messages on the current VLAN.</td>
<td>30 seconds</td>
<td>(page 74)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-sparse hello-delay 0-5 vlan vid ip pim-sparse hello-delay 0-5</td>
<td>Changes the maximum time in seconds before the router actually transmits the initial PIM hello message on the current VLAN.</td>
<td>5 seconds</td>
<td>(page 75)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip pim-sparse lan-prune-delay vlan vid ip pim-sparse lan-prune-delay</td>
<td>Enables the LAN Prune Delay option on the current VLAN.</td>
<td>Enabled</td>
<td>(page 75)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip pim-sparse propagation-delay 250-2000 vlan vid ip pim-sparse propagation-delay 250-2000 ip pim-sparse override-interval 500-6000 vlan vid ip pim-sparse override-interval 500-6000</td>
<td>A router sharing a VLAN with other multicast routers uses these two values to compute the lan-prune-delay setting for how long to wait for a PIM-SM join after receiving a prune packet from downstream for a particular multicast group.</td>
<td></td>
<td>(page 76)</td>
<td>-</td>
</tr>
<tr>
<td>ip pim-sparse dr-priority 0-4294967295</td>
<td>Changes the router priority for the DR election process in the current VLAN.</td>
<td>1</td>
<td>(page 76)</td>
<td>-</td>
</tr>
<tr>
<td>[no] bsr-candidate source-ip-vlan vid [no] router pim bsr-candidate source-ip-vlan vid</td>
<td>Configures the router to advertise itself as a candidate PIM-SM BSR on the VLAN interface specified by source-ip-VLAN vid, and</td>
<td></td>
<td>(page 77)</td>
<td>-</td>
</tr>
</tbody>
</table>
# Table 8 Summary of commands (continued)

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] bsr-candidate router pim bsr-candidate</td>
<td>Disables or re-enables the router for advertising itself as a candidate-BSR on the VLAN interface specified by <code>source-ip-vlan vid</code>.</td>
<td>Disabled</td>
<td>??</td>
<td>-</td>
</tr>
<tr>
<td>bsr-candidate priority 0-255 [no] router pim bsr-candidate priority 0-255</td>
<td>Specifies the priority to apply to the router when a BSR election process occurs in the PIM-SM domain.</td>
<td>0</td>
<td>“??TITLE???” (page 78)</td>
<td>-</td>
</tr>
<tr>
<td>bsr-candidate hash-mask-length 1-32 [no] router pim bsr-candidate hash-mask-length 1 - 32</td>
<td>Controls distribution of multicast groups among the C-RPs in a domain where there is overlapping coverage of the groups among the RPs.</td>
<td>30</td>
<td>bsr-candidate hash-mask-length [1-32]</td>
<td>-</td>
</tr>
<tr>
<td>bsr-candidate bsm-interval 5-300 [no] router pim bsr-candidate bsm-interval 5-300</td>
<td>Specifies the interval in seconds for sending periodic RP-set messages on all PIM-SM interfaces on a router operating as the elected BSR in a domain.</td>
<td>60</td>
<td>“??TITLE???” (page 79)</td>
<td>-</td>
</tr>
<tr>
<td>[no] rp-candidate source-ip-vlan vid [group-prefix group-addr/mask.] [no] router pim rp-candidate source-ip-vlan vid [group-prefix group-addr/mask]</td>
<td>Specifies the source IP VLAN (and optionally configures one or more multicast groups or range of groups)</td>
<td>Disabled</td>
<td>(page 79)</td>
<td>-</td>
</tr>
<tr>
<td>[no] rp-candidate</td>
<td>Enables C-RP operation on the router.</td>
<td>-</td>
<td>(page 81)</td>
<td>-</td>
</tr>
<tr>
<td>[no] rp-candidate group-prefix [group-addr</td>
<td>group-mask ]</td>
<td>Adds a multicast group address to the current C-RP configuration.</td>
<td>-</td>
<td>(page 81)</td>
</tr>
<tr>
<td>rp-candidate hold-time 30-255</td>
<td>Changes the hold time a C-RP includes in its advertisements to the BSR.</td>
<td>150 seconds</td>
<td>(page 82)</td>
<td>-</td>
</tr>
<tr>
<td>rp-candidate priority 0-255</td>
<td>Changes the current priority setting for a C-RP.</td>
<td>192</td>
<td>(page 82)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router pim trap [ all</td>
<td>neighbor-loss</td>
<td>hardware-mrt-full</td>
<td>software-mrt-full ]</td>
<td>Enables and disables PIM SNMP traps.</td>
</tr>
<tr>
<td>router pim join-prune-interval 5-65535</td>
<td>Sets the interval in seconds at which periodic PIM-SM join/prune messages are to be sent on the router’s PIM-SM interfaces.</td>
<td>60 seconds</td>
<td>(page 83)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router pim spt-threshold</td>
<td>When the router is the edge router for a receiver requesting to join a particular multicast group, enables or disables the capability of the router to</td>
<td>Enabled</td>
<td>(page 83)</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 8 Summary of commands (continued)

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] router pim rp-address</td>
<td>Statically configures an RP to accept multicast traffic.</td>
<td>-</td>
<td>(page 83)</td>
<td>-</td>
</tr>
<tr>
<td>rp-ip-addr group-addr/group-mask [override]</td>
<td>convert the group’s traffic from the RPT to the SPT.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] rpf-override</td>
<td>Add, edit or delete up to 8 RPF override entries.</td>
<td>-</td>
<td>(page 85)</td>
<td></td>
</tr>
<tr>
<td>source-ip-addr/mask-length rpf-ip-addr</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip pim rpf-override [source source ip-address]</td>
<td>Displays the configured RPF override entries.</td>
<td></td>
<td>(page 86)</td>
<td></td>
</tr>
<tr>
<td>show ip mroute</td>
<td>Lists data for all VLANs actively forwarding routed, multicast traffic.</td>
<td>-</td>
<td>(page 86)</td>
<td>-</td>
</tr>
<tr>
<td>show ip mroute [group-addr source-addr]</td>
<td>Lists data for the specified flow (multicast group).</td>
<td>-</td>
<td>(page 88)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim</td>
<td>Displays PIM status and global parameters.</td>
<td>-</td>
<td>(page 92)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim mroutew</td>
<td>Shows PIM-specific information from the IP MRT.</td>
<td>-</td>
<td>(page 92)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim interface</td>
<td>Lists the PIM interfaces (VLANs) currently configured in the router.</td>
<td>-</td>
<td>(page 93)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim interface [vid]</td>
<td>Displays the current configuration for the specified VLAN (PIM interface).</td>
<td>-</td>
<td>(page 93)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim neighbor</td>
<td>Lists PIM neighbor information for all PIM neighbors connected to the router.</td>
<td>-</td>
<td>(page 94)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim neighbor [ip-address]</td>
<td>Lists the same information as show ip pim neighbor for the specified PIM neighbor.</td>
<td>-</td>
<td>(page 94)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim bsr</td>
<td>Lists BSR status and configuration data.</td>
<td>-</td>
<td>(page 96)</td>
<td>-</td>
</tr>
<tr>
<td>show ip pim rp-set [ learned</td>
<td>Displays the multicast group support for both the learned (elected) C-RP assignments and any statically configured RP assignments.</td>
<td>-</td>
<td>(page 98)</td>
<td>-</td>
</tr>
<tr>
<td>static ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip pim rp-candidate [config]</td>
<td>Lists the router’s C-RP status and configuration.</td>
<td>-</td>
<td>(page 99)</td>
<td>-</td>
</tr>
</tbody>
</table>

### Configuring router protocol independent multicast (PIM)

For more information, see “Configuration steps for PIM-SM” (page 109).

The following steps configure PIM-SM in the router PIM context (`HP Switch(pim)#`):

- Configure router protocol independent multicast (PIM)
- For more information, see “Configuration steps for PIM-SM” (page 109).
1. Specify the VLAN interface to advertise as the Bootstrap Router (BSR) candidate and enable the router to advertise itself as a candidate BSR in a PIM-SM domain. (Use the command `bsr-candidate source-ip-vlan [vid].`)

2. Optional: To make BSR candidate selection occur quickly and predictably, set a different priority on each BSR candidate in the domain. (Use the command `bsr-candidate priority`.)

3. Do one of the following to configure RP operation:
   - Recommended: Enable Candidate Rendezvous Point (C-RP) operation and configure the router to advertise itself as a C-RP to the BSR for the current domain. This step includes the option to allow the C-RP to be a candidate for either all possible multicast groups or for up to four multicast groups and/or ranges of groups. Use the command `rp-candidate source-ip-vlan [vid] [group-addr/group-mask].`
   - Optional: Use the command `rp-address [ip-addr] [group-addr/group-mask]` to statically configure the router as the RP for a specified multicast group or range of multicast groups. (This must be configured on all PIM-SM routers in the domain.)

4. Optional: In the PIM router context, change one or more of the traffic control settings in the following table.

<table>
<thead>
<tr>
<th>Options accessed in router PIM context</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rp-candidate group-prefix [group-addr/group-mask]</code></td>
<td>Enter an address and mask to define an additional multicast group or a range of groups.</td>
</tr>
<tr>
<td><code>rp-candidate hold-time [30-255]</code></td>
<td>Tells the BSR how long it should expect the sending C-RP router to be operative. Default: 150; 0 if router is not a candidate</td>
</tr>
<tr>
<td><code>rp-candidate priority [0-255]</code></td>
<td>Changes the priority for the C-RP router. When multiple C-RPs are configured for the same multicast groups, the priority determines which router becomes the RP for such groups. A smaller value means a higher priority. Default: 192</td>
</tr>
<tr>
<td><code>[no] spt-threshold (page 83)</code></td>
<td>Disable or enable the router’s ability to switch multicast traffic flows to the shortest path tree. Default: enabled</td>
</tr>
<tr>
<td><code>join-prune-interval [5-65535] (page 74)</code></td>
<td>Option: Globally change the interval for the frequency at which join and prune messages are forwarded on the router’s VLAN interfaces. Default: 60 seconds</td>
</tr>
<tr>
<td>`trap [ neighbor-loss</td>
<td>hardware-mrt-full</td>
</tr>
</tbody>
</table>

**Configuring PIM-SM on the router**

**Global configuration context for supporting PIM-SM**

Before configuring specific PIM-SM settings, it is necessary to enable IP routing, IP multicast routing, an IP routing protocol, and PIM in the global configuration context. Also, if the router operates as an edge router for any endpoints (receivers) expected to join multicast groups, it is also necessary to enable IGMP on the VLANs supporting such receivers.

**Configuring global context commands**

**NOTE:** PIM-SM operation requires an IP routing protocol enabled on the router. You can use RIP, OSPF, and/or static routing. The examples in this section use RIP. See “Routing Basics” (page 116).
Syntax:

```
[no] ip routing
```

Enables IP routing on the router.

The `no` form of the command disables IP routing. Note that before disabling IP routing, it is necessary to disable all other IP routing protocols on the router.

(Default: Disabled)

Syntax:

```
[no] ip multicast-routing
```

Enables or disables IP multicast routing on the router. IP routing must first be enabled. Note that router PIM must be disabled before disabling IP multicast routing.

(Default: Disabled)

Syntax:

```
[no] router [ ospf | rip ]
[no] ip route [ ip-addr/mask-len ] [ ip-addr | vlan | reject | blackhole ]
```

These commands are the options for the IP routing protocol required to support PIM operation. For more on these options, see “Routing Basics” (page 116).

Syntax:

```
[no] router pim [ [enable] | [disable] ]
```

Puts the CLI into the PIM context level. IP routing must be enabled before enabling PIM.

The `no router pim` command deletes the PIM configuration. (Default: Disabled)

[enable]

  Enables PIM globally.

[disable]

  Disables PIM globally. Disabling PIM does not delete the PIM configuration.
Example 31 Configuring for PIM support at the global level

Using the topology (Figure 20 (page 104)), router "B" is directly connected to the DR for multicast group "X." In this case, suppose that you want to globally configure router "B" for PIM operation. On the global level, you would enable the following:

- IP routing
- IP multicast routing
- An IP routing protocol (RIP, OSPF, or static routing; use RIP for this example)

Figure 12 PIM-SM domain with SPT active to support a host that has joined a multicast group

Example 32 Global configuration for supporting PIM-SM operation

```
HP Switch(config)# ip routing
HP Switch(config)# ip multicast-routing
HP Switch(config)# router rip
HP Switch(rip)# exit
HP Switch(config)# router pim
HP Switch(pim)# exit
HP Switch(config)#
```

Figure 13 Displaying the running configuration

```
HP Switch(config)# show running-config
Running configuration:
; J8693A Configuration Editor; Created on release #K.11.XX
hostname "HP Switch"
module 2 type J8705A
module 1 type J8702A
ip routing ]
snmp-server community "public" Unrestricted
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A24, B1-B24
  ip address 10.10.10.1 255.255.255.0
  exit
ip multicast-routing ]
router rip
  exit
router pim
  exit

Global Routing Configuration for PIM-SM Support
Note: Either RIP, OSPF, or static routing can be used for a routing protocol.
```
VLAN context commands for configuring PIM-SM

PIM-SM must be configured on at least one VLAN in the router before it can be configured as a C-BSR or a C-RP.

Enabling or disabling IGMP in a VLAN

IGMP must be enabled in VLANs on edge routers where multicast receivers (end points) are connected and will be requesting to join multicast groups.

Syntax:

```no
ip igmp
no vlan [vid] ip igmp```

Enables or disables IGMP operation in the current VLAN. Configuring IGMP on the router is required in VLANs supporting edge router operation. See Figure 7 (page 42).

Enabling or disabling PIM-SM per-VLAN

Syntax:

```ip pim-sparse [ip-addr [any | ip-addr]]
vlan [vid] ip pim-sparse [ip-addr [any | ip-addr]]
no [vlan [vid]] ip pim-sparse```

This command enables or disables PIM-SM in the designated VLAN interface and sets the source (and designated router) IP address for PIM-SM packets sent from the interface. Executing the command without specifying an IP address option causes the router to default to the any option, below. (Default: PIM-SM disabled)

```ip-addr any```

Enables the router to dynamically determine from the VLAN’s current IP configuration the source IP address to use for PIM-SM packets sent from the VLAN interface.

**NOTE:** Using this command after a source IP address has already been set does not change that setting.

```ip-addr [ip-addr]```

Specifies one of the VLAN’s currently existing IP addresses for use as the source IP address for PIM-SM packets sent from the VLAN interface.

Note that *ip-addr* must first be statically configured on the VLAN.

**NOTE:** To change an existing source IP address setting, you *must* use this command option.

Changing the interval for PIM-SM neighbor notification

Syntax:

```ip pim-sparse hello-interval [5-300]
vlans vid ip pim-sparse hello-interval [5-300]```

Changes the frequency at which the router transmits PIM hello messages on the current VLAN. The router uses hello packets to inform neighbor routers of its presence.

The router 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 router. 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 changes how quickly
other routers will stop sending traffic to the router if they do not receive a new hello
packet when expected. For example, if multiple routers are connected to the same
VLAN and the router requests multicast traffic, all routers on the VLAN receive that
traffic. (Those that have pruned the traffic will drop it when they receive it.) If the
upstream router loses contact with the router receiving the multicast traffic (that is,
fails to receive a hello packet when expected), the shorter hello interval causes it
to stop transmitting multicast traffic onto the VLAN sooner, resulting in less
unnecessary bandwidth use.

(Default: 30 seconds)

Changing the randomized delay setting for PIM-SM neighbor notification

Syntax:

```
ip pim-sparse hello-delay [0-5]
vlan [vid] ip pim-sparse hello-delay [0-5]
```

Changes the maximum time in seconds before the router 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, 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 router 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)

Enabling or disabling lan prune delay

Syntax:

```
[no] ip pim-sparse lan-prune-delay
[no]
vlan [vid] ip pim-sparse lan-prune-delay
```

Enables the LAN prune delay option on the current VLAN. With lan-prune-delay
enabled, the router 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 multicast receivers continuing to belong to the flow
to reply with a join. If no joins are received after the lan-prune-delay period,
the router prunes the flow.

The propagation-delay and override-interval settings (below) determine
the lan-prune-delay setting.

Uses the no form of the command to disable the LAN prune delay option.

(Default: Enabled)
Changing the **Lan-prune-delay** interval

**Syntax:**

```bash
ip pim-sparse propagation-delay [250-2000]
ip pim-sparse override-interval [500-6000]
vlan [vid] ip pim-sparse override-interval [500-6000]
```

A router 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-SM join after receiving a prune packet from downstream for a particular multicast group.

**Example 33 Multiple routers sharing VLAN**

A network may have multiple routers sharing VLAN "X." When an upstream router is forwarding traffic from multicast group "X" to VLAN "Y," if one of the routers 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 router 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, 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)

**Neighbor timeout**

**Syntax:**

```bash
ip pim-sparse nbr-timeout [60-65536]
```

**Changing the DR priority**

**Syntax:**

```bash
ip pim-sparse dr-priority [0-4294967295]
```

This command changes the router priority for the DR election process in the current VLAN. A numerically higher value means a higher priority. If the highest priority is shared by multiple routers in the same VLAN, the router with the highest IP address is selected as the DR.

A 0 (zero) value disables DR operation for the router on the current VLAN.

(Range: 0 - 2147483647; Default: 1)

**Configuring PIM-SM support in a VLAN context**

PIM-SM support must be configured in each VLAN where you want PIM-SM forwarding of multicast traffic. This illustrates the following per-VLAN configuration steps:

- Enabling PIM-SM on VLAN 120 and allowing the default any option to select a source IP address for PIM-SM packets forwarded from this VLAN. (Because the VLAN in this example...
is configured with only one IP address—120.10.10.2—it is this address that will be used for the source.)

- Increasing the DR priority on this VLAN from the default 1 to 100.
- Leaving the other per-VLAN PIM-SM fields in their default settings.

Figure 14 Example of Enabling PIM-SM in a VLAN

Router PIM context commands for configuring PIM-SM operation

This section describes the commands used in the Router PIM context to:

- Enable or disable SNMP trap status for PIM events (default: disabled)
- Configure candidate BSR operation
- Configure C-RP operation or the (optional) static RP operation

**NOTE:** Before configuring BSR, RP, and SNMP trap operation for PIM-SM, it is necessary to enable PIM-SM on at least one VLAN on the router.

Configuring a BSR candidate

Selecting the VLAN interface to advertise as a BSR candidate.

**Syntax:**

```plaintext
[no] bsr-candidate source-ip-vlan [vid]
[no]
router pim bsr-candidate source-ip-vlan [vid]
```

Configures the router to advertise itself as a candidate PIM-SM BSR on the VLAN interface specified by `source-ip-vlan [vid]`, and enables BSR candidate operation. This makes the router eligible to be elected as the BSR for the PIM-SM domain in which it operates. Note that one BSR candidate VLAN interface is allowed per-router. The `no` form of the command deletes the BSR source IP VLAN configuration and also disables the router from being a BSR candidate, if this option has been enabled. (See the `bsr-candidate` command, below.)

Enabling or disabling a BSR Candidate

Enable or disable BSR candidate operation on a router.
Syntax:

```plaintext
[no] bsr-candidate
[no]
router pim bsr-candidate
```

Disables or re-enables the router for advertising itself as a Candidate-BSR on the VLAN interface specified by `source-ip-vlan [vid]`. This command is used to disable and re-enable BSR candidate operation after the `bsr-candidate source-ip-vlan [vid]` command has been used to enable C-BSR operation on the router. (This command operates only after the BSR source-ip-VLAN ID has been configured.)

(Default: Disabled)

**Changing the priority setting**

Changing the priority setting for a BSR-candidate router.

**Syntax:**

```plaintext
bsr-candidate priority [0-255]
[no] router pim bsr-candidate priority [0-255]
```

Specifies the priority to apply to the router when a BSR election process occurs in the PIM-SM domain. The candidate with the highest priority becomes the BSR for the domain. If the highest priority is shared by multiple routers, the candidate having the highest IP address becomes the domain's BSR. Zero (0) is the lowest priority. To make BSR selection easily predictable, use this command to assign a different priority to each candidate BSR in the PIM-SM domain.

(Default: 0; Range 0–255)

**NOTE:** Disabling PIM-SM on the elected BSR or disabling the C-BSR functionality on the elected BSR causes the router to send a Bootstrap Message (BSM) with a priority setting of 0 to trigger a new BSR election. If all BSRs in the domain are set to the default priority (0), the election will fail because the result is to re-elect the BSR that has become unavailable. For this reason, it is recommended that all C-BSRs in the domain be configured with a `bsr-candidate priority` greater than 0.

**Changing the distribution**

Changing the distribution of multicast groups across a domain.

**Syntax:**

```plaintext
bsr-candidate hash-mask-length [1-32]
[no] router pim bsr-candidate hash-mask-length [1-32]
```

Controls distribution of multicast groups among the C-RPs in a domain where there is overlapping coverage of the groups among the RPs. This value specifies the length (number of significant bits) taken into account when allocating this distribution. A longer `hash-mask-length` results in fewer multicast groups in each block of group addresses assigned to the various RPs. Because multiple blocks of addresses are typically assigned to each C-RP, this results in a wider dispersal of addresses and enhances load-sharing of the multicast traffic of different groups being used in the domain at the same time.

(Default: 30; Range 1–32)

**Changing the message interval**

Changing the BSR message interval.
Syntax:

bsr-candidate bsm-interval [5-300]
[no] bsr-candidate bsm-interval [5-300]

Specifies the interval in seconds for sending periodic RP-Set messages on all PIM-SM interfaces on a router operating as the elected BSR in a domain.

**NOTE:** This setting must be smaller than the `rp-candidate hold-time` settings (range of 30 to 255; default 150) configured in the RPs operating in the domain.

(Default: 60; Range 5–300)

**Configuring C-RPs on PIM-SM routers**

An RP candidate advertises its availability, IP address, and the multicast group or range of groups it supports. The commands in this section are used to configure C-RP operation. The sequence of steps is as follows:

1. Specify the source IP VLAN.
2. Enable C-RP operation.
3. Option: enable or disable specific multicast address groups.

**NOTE:** Before configuring BSR, RP, and SNMP trap operation for PIM-SM, it is necessary to enable PIM-SM on at least one VLAN on the router.

**Specifying the source IP VLAN (and optionally configuring one or more multicast groups or range of groups)**

Specifying the source IP VLAN ID automatically configures the C-RP to support all multicast groups (unless you include an individual group or range of groups in the command). The recommended approach is to allow all multicast groups unless you have a reason to limit the permitted groups to a specific set.

**Syntax:**

[no] rp-candidate source-ip-vlan [vid] [group-prefix group-addr/mask]
[no] router pim rp-candidate source-ip-vlan [vid] [group-prefix group-addr/mask]
These commands configure C-RP operation in the following way.

- Specify the VLAN interface from which the RP IP address will be selected for advertising the router as an RP candidate.

  **NOTE:** Only one VLAN on the router can be configured for this purpose at any time.

- Enable the router as an RP candidate.

- Specify the multicast groups for which the router is a CRP. (Default: Disabled.)

  **NOTE:** When executed without specifying a multicast group or range of groups, the resulting RP candidate defaults to allow support for all multicast groups — 224.0.0.0 240.0.0.0, or 224.0.0.0/4.

Additionally, the following commands may be required:

- To later add to or change multicast groups, or to delete multicast groups, use the command `rp-candidate group-prefix [group-addr | group-mask]`. See “Adding or deleting a multicast group address” (page 81).

- To disable C-RP operation without removing the current CRP configuration, use the command `no rp-candidate`. See “Enabling or disabling C-RP operation” (page 81).

- The `no` form of these commands:
  - Deletes the RP source IP VLAN configuration.
  - Deletes the multicast group assignments configured on the router for this RP.
  - Disables the router from being an RP candidate.

  `[vid]`
  The command identifies the VLAN source of the IP address to advertise as the RP candidate address for the router.

  `group-prefix [group-addr/mask]`:
  Specifies the multicast group(s) to advertise as supported by the RP candidate. Use this option when you want to enable the C-RP and simultaneously configure it to support a subset of multicast addresses or ranges of addresses instead of all possible multicast addresses.

  A group prefix can specify all multicast groups (224.0.0.0 to 239.255.255.255), a range (subset) of groups, or a single group. A given address is defined by its nonzero octets and mask. The mask is applied from the high end (leftmost) bits of the address and must extend to the last nonzero bit in the lowest-order, nonzero octet. Any intervening zero or nonzero octet requires eight mask bits. Following are examples.
Example 34 228.0.0.64/26:
Defines a multicast address range of 228.0.0.64 through 228.0.0.127. (The last six bits of the rightmost octet are wildcards.)

Example 35 228.0.0.64/30:
Defines a multicast address range of 228.0.0.64 through 228.0.0.67. (The last two bits of the rightmost octet are wildcards.)

Example 36 228.0.0.64/32:
Defines a single multicast address of 228.0.0.64. (There are no wildcards in this group prefix.)

Example 37 228.0.0.64/25:
Creates an error condition caused by the mask failing to include the last (rightmost) nonzero bit in the lowest-order, nonzero octet. (That is, this mask supports an address of 228.0.0.128, but not 228.0.0.64.)

NOTE: The larger the mask, the smaller the range of multicast addresses supported. A mask of 32 bits always specifies a single multicast address. For example 230.0.15.240/32 defines a single multicast address of 230.0.15.240.

Enabling or disabling C-RP operation
Use this command when the router is already configured with a source IP VLAN ID and you want to enable or disable C-RP operation on the router.

Syntax:

[no]rp-candidate
Enables C-RP operation on the router. Requires that the source IP VLAN is currently configured, but disabled. See (page 79).
The no form of the command disables the currently configured C-RP operation, but does not change the configured C-RP settings.

Adding or deleting a multicast group address
Use this command if you need to modify the multicast address group configuration for a C-RP on the router.

Syntax:

[no]rp-candidate group-prefix [ group-addr | group-mask ]
Adds a multicast group address to the current C-RP configuration. Requires that the source IP VLAN (See 79) is already configured. The no form of the command removes a multicast group address from the current C-RP configuration.
This command does not enable or disable RP candidate operation.

NOTE: An RP candidate supports up to four separate multicast address groups. If only one group-prefix address exists in the router PIM configuration, you cannot delete it unless you first add another group-prefix address.
Changing the C-RP hold-time

Hold-time is included in the advertisements the C-RP periodically sends to the domain’s elected BSR, and updates the BSR on how long to wait after the last advertisement from the reporting RP before assuming that it has become unavailable. See “BSR role in fault recovery” (page 106).

Syntax:

```
rp-candidate hold-time [30-255]
```

Changes the hold time a C-RP includes in its advertisements to the BSR. Also, if C-RP is configured, but disabled, this command re-enables it.

(Default: 150 seconds; Range: 30–255 seconds.)

Changing a C-RP's election priority

This priority is significant when multiple C-RPs in a given domain are configured to support one or more of the same multicast groups.

Syntax:

```
rp-candidate priority [0-255]
```

Changes the current priority setting for a C-RP. Where multiple C-RPs are configured to support the same multicast group(s), the candidate having the highest priority is elected. Zero (0) is the highest priority, and 255 is the lowest priority.

(Default: 192)

Enabling, disabling, or changing router PIM notification traps

Syntax:

```
[no] router pim trap [ all | neighbor-loss | hardware-mrt-full | software-mrt-full ]
```

Enables and disables the following PIM SNMP traps:

- **all**
  - Enable/Disable all PIM notification traps.
  - (Default: Disabled)

- **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 sent when the hardware multicast routing table (MRT) is full (2048 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 sent when the router’s software MRT is full (that is, when routing resources for active flows are exhausted). Note that in this state, the router does not accept any additional flows.
  - (Default: Disabled)
NOTE: Trap operation requires configuring an SNMP trap receiver by using the `snmp-server host [ip-addr]` command at the global configuration level.

Changing the global join-prune interval on the router

Syntax:

```
router pim join-prune-interval [5-65535]
```

Sets the interval in seconds at which periodic PIM-SM join/prune messages are to be sent on the router's PIM-SM interfaces. This setting is applied to every PIM-SM interface on the router.

(Default: 60 seconds)

NOTE: All routers in a PIM-SM domain should have the same join-prune-interval setting.

Changing the shortest-path tree (SPT) operation

Generally, using the SPT option eliminates unnecessary levels of PIM-SM traffic in a domain. However, in cases where it is necessary to tightly control the paths used by PIM-SM flows to edge switches, disabling SPT maintains the flows through their original C-RPs regardless of whether shorter paths exist.

Syntax:

```
router pim spt-threshold [no] router pim spt-threshold
```

When the router is the edge router for a receiver requesting to join a particular multicast group, this command enables or disables the capability of the router to convert the group's traffic from the RPT to the SPT.

See “Restricting multicast traffic to RPTs” (page 104).

(Default: Enabled)

Statically configuring an RP to accept multicast traffic

A given static RP entry should be manually configured on all routers in the PIM-SM domain. See “Static RP (static RP)” (page 107).

Syntax:

```
router pim rp-address [rp-ip-addr] [group-addr/group-mask] [override] [no] router pim rp-address [rp-ip-addr] [group-addr/group-mask] [override] [rp-ip-addr]
```

Statically specifies the IP address of the interface to use as an RP. Up to eight static RP IP addresses can be configured. (Each address can be entered multiple times for different multicast groups or group ranges.)

```
[group-addr/group-mask]
```

Specifies the multicast group or range of contiguous groups supported by the statically configured RP. Up to eight multicast group ranges can be configured.

```
[override]
```

Where a static RP and a C-RP are configured to support the same multicast group(s) and the multicast group mask for the static RP is equal to or greater
than the same mask for the applicable C-RPs, this command assigns the higher precedence to the static RP, resulting in the C-RP operating only as a backup RP for the configured group. Without override, the C-RP has precedence over a static RP configured for the same multicast group(s).

Configuring PIM-SM support in the router PIM context

This example assumes the following:

- IP routing, IP multicast routing, and at least one routing method (RIP, OSPF, and/or static IP routes) are already configured in the global configuration context.
- An IP routing method (RIP or OSPF) and PIM-sparse are already configured in the static VLAN context on which you want to support PIM-SM operation.

**NOTE:** Routers configured for C-RP operation can also be configured for C-BSR operation. Use of static RP operation must be identically configured on all PIM-SM routers in the domain.

Figure 15 (page 84) illustrates the following configuration steps for the router PIM context:

- Enabling BSR operation on the router, including specifying a source IP address.
- Enabling C-RP operation on the router.
- Replacing the default multicast group range (all) with a smaller range (231.128.24.0/18) and a single group address (230.255.1.1/32).
- Enabling static RP with an override on this router for a single group address (231.128.64.255/32) within the range of the C-RP support for the 231.128.24.0 group.
- Leaving the other router PIM fields in their default settings.

**Figure 15 Example of enabling PIM-SM in the router PIM context**

The next figure illustrates the results of the above commands in the router’s running configuration.
Configuring PIM RPF override

Overview

Reverse Path Forward (RPF) checking is a core multicast routing mechanism that ensures that multicast traffic received arrived on the expected router interface before it is considered for further processing. If the RPF check fails for a multicast packet, the packet is discarded.

For traffic arriving on the SPT, the expected incoming interface for a given source/group multicast flow is the interface towards the source address of the traffic (as determined by the unicast routing system). For traffic arriving on the RP tree, the expected incoming interface is the interface towards the RP.

RPF override is an HP networking feature that allows the override of the normal RPF lookup mechanism and indicates to the router that it may accept multicast traffic on an interface other than that which would be normally selected by the RPF lookup mechanism. This includes accepting traffic from a source directly connected to the router when the source IP address is invalid for the subnet or VLAN to which it is connected. Traffic may also be accepted from a valid PIM neighbor that is not on the reverse path towards the source of the received multicast traffic.

RPF checking is applied to all multicast traffic and is significant in preventing network loops. Up to eight manual RPF overrides can be specified.

NOTE: These static RPF override entries are not distributed.

The manually configured static multicast RPF override is restored on subsequent reboots. The command is executed in PIM context.

Syntax:

```text
[no] rpf-override [source-ip-addr/mask-length] [rpf-ip-addr]
```

Add, edit, or delete up to eight RPF override entries. The multicast RPF override has a multicast source address `[source-ip-addr/mask-length]` and an RPF address `[rpf-ip-addr]` pair. The `no` form of the command deletes the RPF override.

NOTE: Only host-specific addresses are supported (i.e. “/32” addresses).

```text
[source-ip-addr]
The IPv4 address of the host from which the multicast flow originated.
```

```text
[mask-length]
The length, in bits, of the mask used to indicate the range of addresses from `[source-ip-addr]` to which the RPF override command applies. Currently, only a 32-bit mask is supported, that is, only one host per entry. Eight individual entries are supported.
```
The IPv4 address indicating one of two distinct RPF candidates:

1. A valid PIM neighbor address from which forwarded multicast traffic is accepted with a source address of [source-ip-addr].

2. A local router address on a PIM-enabled VLAN to which [source-ip-addr] is directly connected. The local router will assume the role of DR for this flow and registers the flow with an RP, if configured.

**Example 39 Configuring a manual multicast RPF override and saving it in the config**

```
HP Switch(config)# ip routing
HP Switch(config)# ip multicast-routing
HP Switch(config)# router pim
HP Switch(pim)# rpf-override 10.1.1.1/32 11.2.2.1
HP Switch(pim)# write mem
```

**Displaying configured RPF overrides**

You can display the configured RPF overrides with the `show` command.

**Syntax:**

```
show ip pim rpf-override [source | source ip-address]
```

Displays the configured RPF override entries.

```
[source ip-address]
```

Displays the RPF overrides for a specific IP address. This can be useful when troubleshooting potential RPF misconfigurations.

**Example:**

**Example 40 Displaying the configured RPF overrides**

```
HP Switch(config)# show ip pim rpf-override
Static RPF Override
Multicast Source    RPF IP Address
------------------- ---------------
10.1.1.1/32         11.2.2.1
13.1.1.1/32         12.1.1.1
```

**Example 41 Specifying the source parameter to troubleshoot misconfigurations**

```
HP Switch(config)# show ip pim rpf-override source 10.1.1.1
Static RPF Override
Multicast Source    RPF IP Address
------------------- ---------------
10.1.1.1/32         11.2.2.1
```

**Displaying PIM route data**

The commands in this section display multicast routing information on packets sent from multicast sources to IP multicast groups detected by the routing switch.

**Listing basic route data for active multicast groups**

**Syntax:**

```
show ip mroute
```
Lists the following data for all VLANs actively forwarding multicast traffic, or for VLANs receiving registered but non-forwarding traffic on an RP.

**Group Address**
- The multicast group IP address of the specific flow (source-group pair).

**Source Address**
- The unicast address of the flow's 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 router.

**VLAN**
- The interface on which the router received the multicast flow.

**Example**
The following figures display the `show ip mroute` output illustrating three different cases:
Example 42 Showing source-DR PIM router

Source-DR PIM router. A flow’s Neighbor field is empty for a PIM Router with a directly connected source.

```
HP Switch(config)# show ip mroute
IP Multicast Route Entries
Total number of entries : 1
Group Address       Source Address   Neighbor     VLAN
------------------- --------------- ----------- ----
239.255.11.1        10.0.0.10        -----------   20
```

Example 43 Showing intermediate PIM router

Flows show their adjacent PIM neighbor towards the source.

```
HP Switch(config)# show ip mroute
IP Multicast Route Entries
Total number of entries : 2
Group Address       Source Address   Neighbor     VLAN
------------------- --------------- ----------- ----
239.255.12.42       10.0.0.10        20.0.0.1     20
239.255.255.255     10.0.0.10        20.0.0.1     20
```

Example 44 Showing new RP special case

RP special case: When run on a RP, registered but non-forwarding flows are displayed without a neighbor value. This is identical in appearance to a direct-connected source, but on an RP this indicates the unique registered, non-forwarding condition.

```
HP Switch(config)# show ip mroute
IP Multicast Route Entries
Total number of entries : 2
Group Address       Source Address   Neighbor     VLAN
------------------- --------------- ----------- ----
239.255.12.42       10.0.0.10        20.0.0.1     20
239.255.5.20         10.0.0.10        -----------   20
```

Listing data for an active multicast group

**Syntax:**

```
show ip mroute [group-addr] [source-addr]
```

Lists data for the specified multicast flow (single-group pair).

**Data output list**

- **Group address**: The multicast group IP address for the specific flow.
- **Source address**: The source IP address for the specific flow.
- **Neighbor**: Lists the IP address of the upstream next-hop router running PIM-SM; that is, the router from which the router is receiving datagrams for the current multicast group. This value is 0.0.0.0 if the router has not detected the upstream next-hop router’s IP address. This field is empty if the multicast server is directly connected to the router.
- **VLAN**: The interface on which the router received the multicast flow.
Up time (sec)
The elapsed time in seconds since the router learned the information for the current instance of the indicated multicast flow. Note that on an Originator router when a forwarding flow moves to a non-forwarding state (i.e. when pruned) the Up time value for that flow is reset to 0.

Expire Time (sec)
An mroute which is in a forwarding state — one which represents an active, connected flow for which there are downstream routers and/or locally connected hosts interested in the flow — does not expire. When other PIM-SM routers or locally connected hosts are no longer interested in an active flow, the related mroute on a DR moves to a blocking state, and an mroute in this state does not expire either. In both cases the mroute is only removed from the system when it is no longer needed and so the displayed value for expire time in these situations is not meaningful.

For an mroute on a DR router whose flow is no longer active — including mroutes on non-DR routers whose flow has been pruned — expire time indicates when the mroute entry will eventually be cleared.

Note that flows that are registered with an RP router but are not connected downstream (one for which there is no entry displayed in the neighbor field on the RP) will also have an mroute entry that does not expire.

Multicast routing protocol
Identifies the IP multicast routing protocol through which the current flow was learned.

Unicast routing protocol
Identifies the IP routing protocol through which the router learned the upstream interface for the current multicast flow. The listed protocol will be one of connected, static, rip, ospf or other.

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 router 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 router assumes it is the best path, and the specified multicast group traffic will flow through the router.

RPT-tree
A Yes setting indicates the route is using the RPT. A No setting indicates the route is using the applicable SPT.

Downstream interfaces
For each downstream interface the following information is shown:
VLAN
Lists the vid of the VLAN the router 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 router has not detected any joins from the current multicast flow and is not currently forwarding datagrams in the current VLAN.

Forwarding
The router 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 router learned the displayed information about the current multicast flow.

Expire Time (sec)
Downstream interface entries for an mroute in PIM-SM are only created when those interfaces become joined for the mroute’s flow. Unless join state is periodically refreshed, a downstream interface will eventually move from forwarding to pruned. When forwarding, Expire Time indicates when the router expects forwarding to end unless another join for the flow is received. After moving to prune state, the downstream interface entry will last for a short while longer, indicated by Expire Time, before being removed completely.
Example

Example 45 Route entry data for a specific multicast group

The neighbor field indicates that the router is receiving multicast traffic from a neighboring PIM router. A blank neighbor field indicates that the multicast source is directly connected to the router instead of another PIM router.

HP Switch(config)# show ip mroute 239.255.12.42 10.0.0.10

IP Multicast Route Entry
Group Address : 239.255.12.42
Source Address : 10.0.0.10
Neighbor :
VLAN : 10
Up Time (sec) : 940
Expire Time (sec) : 285
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol : Connected
Metric : 1
Metric Pref : 0
Assert Timer : 0
RP tree : No

Downstream Interfaces
VLAN State Up Time (sec) Expire Time (sec)
--- ---------- ----------------- ------------------
20 forwarding 940 204

Example 46 Showing route entry data for a registered, non-forwarding flow

Blank neighbor and unicast routing protocol fields indicate the special registered, non-forwarding RP condition.

HP Switch(config)# show ip mroute 239.255.12.42 10.0.0.10

IP Multicast Route Entry
Group Address : 239.255.12.42
Source Address : 10.0.0.10
Neighbor :
VLAN : 20
Up Time (sec) : 0
Expire Time (sec) : 0
Multicast Routing Protocol : PIM-SM
Unicast Routing Protocol :
Metric : 0
Metric Pref : 0
Assert Timer : 0
RP tree : No

Downstream Interfaces
VLAN State Up Time (sec) Expire Time (sec)
--- ---------- ----------------- ------------------

Listing all VLANs having currently active PIM flows

Syntax:

show ip mroute interface [vid]

This command displays exactly the same output as the command show ip pim interface vid (See “Listing currently configured PIM interfaces” (page 93)).

Displaying PIM-specific data

The commands in this section display PIM-specific multicast routing information for IP multicast groups detected by the router.
Displaying the current PIM status and global configuration

Syntax:

show ip pim

Displays PIM status and global parameters.

- **PIM Status**
  - Shows either **Enabled** or **Disabled**.

- **State Refresh Interval (sec)**
  - Applies only to PIM-DM operation. See “Displaying PIM Status” (page 92).

- **Join/Prune Interval**
  - Indicates the frequency with which the router transmits join and prune messages for the multicast groups the router is forwarding.

- **SPT Threshold**
  - When **Enabled**, indicates that, for a given receiver joining a multicast group, an edge router changes from the RPT to the SPT after receiving the first packet of a multicast flow intended for a receiver connected to the router.
  - When **Disabled**, indicates that the no spt-threshold command has been used to disable SPT operation. (See “Changing the shortest-path tree (SPT) operation” (page 83).)

- **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 table (MRT) is full (2048 active flows).
    - **software-mrt-full**: Sends a trap if the software multicast router table (MRT) is full (2048 active flows). This can occur only if the hardware MRT is also full.
    - **all**
      - Enables all of the above traps.
    - **none**
      - No traps are set.

**Example**

**Example 47 Output with PIM enabled**

```plaintext
HP Switch(config)# show ip pim
PIM Global Parameters
  PIM Status : Enabled
  State Refresh Interval (sec) : 60
  Join/Prune Interval (sec) : 60
  SPT Threshold : Enabled
  Traps : all
```

Displaying current PIM entries existing in the multicast routing table

Syntax:

show ip pim mroute

92  PIM-SM (Sparse Mode)
This command displays exactly the same output as the command `show ip mroute`. (See “Displaying PIM route data” (page 86).)

Listing currently configured PIM interfaces

Syntax:

show ip pim interface

Lists the PIM interfaces (VLANs) currently configured in the router.

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` or `sparse`, depending on which PIM protocol is configured on the router.

Example

**Example 48 Two configured PIM interfaces**

```
HP Switch(config)# show ip pim interface
PIM Interfaces
   VLAN  IP Address      Mode
   ----  --------------- ------------
       1    10.1.10.1       sparse
       2    10.2.10.1       sparse
```

Displaying IP PIM VLAN configurations

Syntax:

show ip pim interface [vid]

Displays the current configuration for the specified VLAN (PIM interface). See Table 9 (page 93).

**Table 9 PIM interface configuration settings**

<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><code>vlan vid ip pim</code></td>
</tr>
<tr>
<td>IP</td>
<td>N/A</td>
<td><code>vlan vid ip pim all</code> <code>ip-addr</code></td>
</tr>
<tr>
<td>Mode</td>
<td>dense</td>
<td><code>n/a; PIM Dense only</code></td>
</tr>
<tr>
<td>Hello interval (sec)</td>
<td>300</td>
<td><code>ip pim hello interval 5 - 30</code></td>
</tr>
<tr>
<td>Hello delay</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>override interval (msec)</td>
<td>2500</td>
<td><code>vlan vid ip pim override-interval 500 - 6000</code></td>
</tr>
</tbody>
</table>
### Table 9 PIM interface configuration settings (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Default</th>
<th>Control command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propagation delay (msec)</td>
<td>500</td>
<td><code>vlan vid ip pim propagation-delay 250-2000</code></td>
</tr>
<tr>
<td>LAN prune delay</td>
<td>Yes</td>
<td><code>vlan vid ip pim lan-prune-delay</code></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>DR priority</td>
<td>1</td>
<td><code>ip pim-sparse dr-priority 0 - 4294967295</code></td>
</tr>
</tbody>
</table>

### Example

**Example 49 Showing a PIM-SM interface configured on VLAN 1**

```
HP Switch(config)# show ip pim interface 1
PIM Interface
VLAN       : 1
IP Address : 10.1.10.1
Mode       : sparse
    Designated Router : 10.1.10.1
Hello Interval (sec) : 30
Hello Delay (sec)    : 5
Override Interval (msec) : 2500     Lan Prune Delay           : Yes
Propagation Delay (msec) : 500      Lan Delay Enabled         : No
Neighbour Timeout        : 180      DR Priority               : 1
```

### Displaying PIM neighbor data

These commands enable listings of either all PIM neighbors the router detects or the data for a specific PIM neighbor.

**Syntax:**

```
show ip pim neighbor
```

Lists PIM neighbor information for all PIM neighbors connected to the router:

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

- **VLAN**
  - Lists the VLAN through which the router connects to the indicated neighbor.

- **Up Time**
  - Shows the elapsed time during which the neighbor has maintained a PIM route to the router.

- **Expire Time**
  - Indicates how long before the router 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.

**DR Priority**

Shows the currently configured priority for DR operation on the interface.

---

**Example**

**Example 50 Listing of all PIM neighbors detected**

```
HP Switch(config)# show ip pim neighbor
PIM Neighbors
<table>
<thead>
<tr>
<th>IP Address</th>
<th>VLAN</th>
<th>Up Time (sec)</th>
<th>Expire Time (sec)</th>
<th>DR Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.2</td>
<td>100</td>
<td>348</td>
<td>90</td>
<td>1</td>
</tr>
<tr>
<td>10.20.10.1</td>
<td>200</td>
<td>410</td>
<td>97</td>
<td>1</td>
</tr>
</tbody>
</table>
```

**Syntax:**

```
show ip pim neighbor [ip-address]
```

Lists the same information as `show ip pim neighbor`. See “Displaying PIM neighbor data” (page 94).

---

**Example**

**Example 51 Output for a specific PIM neighbor**

```
HP Switch(config)# show ip pim neighbor 10.10.10.2
PIM Neighbor
  IP Address : 10.10.10.2
  VLAN       : 100
  Up Time (sec) : 678
  Expire Time (sec) : 93
  DR Priority : 1
```

---

**Display pending join requests**

Use the `show ip pim pending` command to display the pending joins on a PIM router. A pending join can be an IGMPv2 join (host join) or PIM (*,G) or (S,G) join (PIM router joins, PIM-SM only) received by a router for which there is no active multicast flow to satisfy the received join. This aids in determining what flows are being requested on the PIM network, but for which there is no data. If data availability is expected for a flow, and a join for that flow is showing as pending, this moves the troubleshooting search to the source of the flow since the routers are verified to be seeing the request for data.

**Syntax:**

```
show ip pim pending [ip-address]
```

Displays the joins received on the switch from downstream devices that want to join a specified (*,G) or (S,G) multicast group (flow) address or all multicast groups known on the switch.

A join remains in a pending state until traffic is received for the flow. The VLAN (PIM interface) on which each join was received is also displayed.
Incoming VLAN
ID on which a join request is received.

Source IPv4 Address
IP address of the source of multicast traffic in an (S,G) group.

Example Show IP PIM pending command

Syntax
show ip pim rp-pending [ip-address]

Displays the joins received on the switch from downstream devices that want to listen to the multicast traffic in all (*,G) or (S,G) multicast groups (flows) that a specified RP address or all RPs in the domain are responsible for. A join remains in a pending state until traffic is received for the flow. The VLAN (PIM interface) on which each join was received is also displayed.

Incoming VLAN
VLAN ID from which a join request is received.

Source IPv4 Address
IP address of the source of multicast traffic in an (S,G) group.

Displaying BSR data
The router provides BSR information through both IP PIM and the running configuration.

Displaying BSR status and configuration

Syntax:
show ip pim bsr

Lists the identity, configuration, and time data of the currently elected BSR for the domain, plus the BSR-candidate configuration, the C-RP configuration, and the supported multicast groups on the current router.
Figure 16 Listing BSR data for the domain and the immediate router

Listing non-default BSR configuration settings

The `show running` command includes the current non-default BSR configuration settings on the router.
Figure 17 Non-default BSR configuration listing

Example of Non-Default BSR Candidate Configuration in the Router’s Running Configuration

Note: priority appears only if it is configured to a non-default value.

Displaying the current RP set

The BSR sends periodic RP updates to all C-RPs in the domain. These updates include the set of multicast group data configured on and reported by all C-RPs in the domain. This data does not include any static RP entries configured on any router in the domain. (To view the static RP-set information for any static RPs configured on a particular router, you must access the CLI of that specific router.)

Syntax:

show ip pim rp-set [ learned | static ]

Without options, this command displays the multicast group support for both the learned C-RP assignments and any statically configured RP assignments.

learned

Displays only the learned C-RP assignments the router has learned from the latest BSR message.

static

Displays only the statically configured RP assignment(s) configured on the router.
Examples

Example 52 Listing both the learned and static RP-set data

```
HP Switch(config)# show ip pim rp-set
Status and Counters - PIM-SM Static RP-Set Information
<table>
<thead>
<tr>
<th>Group Address</th>
<th>Group Mask</th>
<th>RP Address</th>
<th>Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>231.100.128.255</td>
<td>255.255.255.255</td>
<td>100.10.10.1</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Status and Counters - PIM-SM Learned RP-Set Information
<table>
<thead>
<tr>
<th>Group Address</th>
<th>Group Mask</th>
<th>RP Address</th>
<th>Hold Time</th>
<th>Expire Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>231.100.128.0</td>
<td>255.255.240.0</td>
<td>100.10.10.1</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>232.240.255.252</td>
<td>255.255.255.252</td>
<td>100.10.10.1</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>237.255.248.1</td>
<td>255.255.255.255</td>
<td>100.10.10.1</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>239.10.10.240</td>
<td>255.255.255.240</td>
<td>120.10.10.2</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>239.10.10.240</td>
<td>255.255.255.252</td>
<td>120.10.10.2</td>
<td>150</td>
<td>150</td>
</tr>
</tbody>
</table>
```

The static RP-set applies only to the current routing switch.
The Yes override indicates that the static-RP has precedence over any C-RP routers for supporting the indicated group.

The Learned RP-set is received from the BSR and includes an aggregation of reports it has received from all accessible C-RPs in the domain.

Example 53 Displaying only the learned RP-set data for the PIM-SM domain

```
HP Switch(config)# show ip pim rp-set learned
Status and Counters - PIM-SM Learned RP-Set Information
<table>
<thead>
<tr>
<th>Group Address</th>
<th>Group Mask</th>
<th>RP Address</th>
<th>Hold Time</th>
<th>Expire Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>231.100.128.0</td>
<td>255.255.240.0</td>
<td>100.10.10.1</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>232.240.255.252</td>
<td>255.255.255.252</td>
<td>100.10.10.1</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>237.255.248.1</td>
<td>255.255.255.255</td>
<td>100.10.10.1</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>239.10.10.240</td>
<td>255.255.255.240</td>
<td>120.10.10.2</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td>239.10.10.240</td>
<td>255.255.255.252</td>
<td>120.10.10.2</td>
<td>150</td>
<td>150</td>
</tr>
</tbody>
</table>
```

Example 54 Displaying only the static RP-set data (applies to current router only)

```
HP Switch(config)# show ip pim rp-set static
Status and Counters - PIM-SM Static RP-Set Information
<table>
<thead>
<tr>
<th>Group Address</th>
<th>Group Mask</th>
<th>RP Address</th>
<th>Override</th>
</tr>
</thead>
<tbody>
<tr>
<td>231.100.128.255</td>
<td>255.255.255.255</td>
<td>100.10.10.1</td>
<td>Yes</td>
</tr>
</tbody>
</table>
```

Displaying C-RP data

Displaying the router's C-RP status and configuration

Syntax:
```
show ip pim rp-candidate [config]
  rp-candidate
    Lists the current C-RP status and, if the status is enabled for C-RP operation, includes the current C-RP configuration on the router.
    rp-candidate config
    Lists the current C-RP status and the current C-RP configuration on the router, regardless of whether C-RP operation is currently enabled.
```
Examples

Example 55 Listing for a router that is not configured as a C-RP

HP Switch(pim)# show ip pim rp-candidate
This system is not a Candidate-RP

Example 56 Full C-RP configuration listing

```
HP Switch(pim)# show ip pim rp-candidate config
Status and Counters - PIM-SM C-RP Information
  C-RP Admin Status : This system is not a C-RP
  C-RP Address : 120.10.10.2
  C-RP Hold Time : 150
  C-RP Advertise Period : 60
  C-RP Priority : 192
  C-RP Source IP VLAN : 120

  Group Address   Group Mask
----------------- ---------------
  239.10.10.240   255.255.255.252
```

Example of a C-RP configuration for supporting multicast groups in the range of 239.10.10.240 to 239.10.10.243.

Listing non-default C-RP configuration settings

The `show running` command includes the current non-default C-RP configuration settings on the router.

Figure 18 Non-default C-RP configuration listing

```
HP Switch(config)# show running
Running configuration:
  ...  
ip routing
  ...  
  snmp-server community "public" Unrestricted
vlan 1 
  .
  .
vlan 120 
  .
  .
ip multicast-routing
router rip
  .
exit
router pim
  bsr-candidate
    bsr-candidate source-ip-vlan 120
    bsr-candidate priority 1
  rp-candidate
    [rp-candidate source-ip-vlan 120
      rp-candidate group-prefix 224.0.0.0 240.0.0.0
      rp-candidate hold-time 150
    ]
  exit
vlan 120
  ip rip 120.10.10.2
  ip pim-sparse
    ip-addr any
    .
    .
```

Example of Non-Default C-RP Configuration in the Router’s Running Configuration
PIM-SM overview

In a network where IP multicast traffic is transmitted for multimedia applications, such traffic is blocked at routed interface (VLAN) boundaries unless a multicast routing protocol is running. Protocol Independent Multicast (PIM) is a family of routing protocols that form multicast trees to forward traffic from multicast sources to subnets that have used a protocol such as IGMP to request the traffic. PIM relies on the unicast routing tables created by any of several unicast routing protocols to identify the path back to a multicast source (reverse path forwarding, or RPF). With this information, PIM sets up the distribution tree for the multicast traffic. The PIM-DM and PIM-SM protocols on the switches covered in this guide enable and control multicast traffic routing.

IGMP provides the multicast traffic link between a host and a multicast router running PIM-SM. Both PIM-SM and IGMP must be enabled on VLANs whose member ports have directly connected hosts with a valid need to join multicast groups.

PIM-DM (See “PIM-DM (Dense Mode)” (page 38)) is used in networks where, at any given time, multicast group members exist in relatively large numbers and are present in most subnets. However, using PIM-DM in networks where multicast sources and group members are sparsely distributed over a wide area can result in unnecessary multicast traffic on routers outside the distribution paths needed for traffic between a given multicast source and the hosts belonging to the multicast group. In such networks, PIM-SM can be used to reduce the effect of multicast traffic flows in network areas where they are not needed. And because PIM-SM does not automatically flood traffic, it is a logical choice in lower bandwidth situations.

License requirements:

In the 3500yl and 5400zl switches, PIM-SM is included with the Premium License. In the 6200yl and 8200zl switches, this feature is included with the base feature set.

PIM-SM features

PIM-SM on the switches covered in this guide include:

Routing protocol support

PIM uses whichever IP unicast routing protocol is running on the router. These can include:

- RIP
- OSPF
- Static routes
- Directly connected interfaces

VLAN interface support:

Up to 127 outbound VLANs (and 1 inbound VLAN) are supported in the multicast routing table (MRT) at any given time. This means the sum of all outbound VLANs across all current flows on a router 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.)

Flow capacity:

Up to 2048 flows are supported in hardware across a maximum of 128 VLANs. (A flow is composed of an IP source address and an IP multicast group address, regardless of the number of active hosts belonging to the multicast group at any given time.)

Multicast group to RP mapping:

PIM-SM uses the BSR protocol to automatically resolve multicast group addresses to C-RP routers. In the current software release, a router administers BSR operation on a PIM-SM domain basis. (BSR zones and PIM border router operation are not currently supported by the switches covered in this guide.) Note that BSR operation does not extend to statically configured RPs. (For more on this topic, see “Static RP (static RP)” (page 107).)
IGMP compatibility:
PIM-SM is compatible with IGMP version 2, and is fully interoperable with IGMP for determining multicast flows.

VRRP:
PIM-SM is fully interoperable with VRRP to quickly transition multicast routes in the event of a failover.

MIB support on the switches covered in this guide:
With some exceptions, PIM-SM supports the parts of the multicast routing MIB (RFC 2932) applicable to PIM-SM operation. (See “Exceptions to Support for RFC 2932 - Multicast Routing MIB” (page 66)).

PIM draft specifications:
Compatible with PIM-SM specification (RFC 4061).

BSR implementation:
Complies with RFC 5059 (scope zones are not supported.)

PIM-SM operation and router types
Unlike PIM-DM, PIM-SM assumes that most hosts do not want to receive multicast traffic, and uses a non-flooding multicast model to direct traffic for a particular multicast group from the source to the VLAN(s) where there are multicast receivers that have joined the group. As a result, this model sends traffic only to the routers that specifically request it.

PIM-SM operation
In a given PIM-SM domain, routers identified as DRs, RPs, and a BSR participate in delivering multicast traffic to the IP multicast receivers that request it. This approach avoids the flooding method of distributing multicast traffic (employed by PIM-DM) and is best suited for lower bandwidth situations.

The software supports the following operation to enable multicast traffic delivery within a PIM-SM domain:
• From a pool of eligible DR candidates in each VLAN, one DR is elected for each VLAN interface having at least one PIM-SM router. In a multinetted domain, this DR supports multicast traffic from a source on any subnet in the VLAN.
• From a pool of eligible BSR candidates in the domain, one BSR is elected for the entire domain.
• From a pool of eligible C-RPs, one is elected to support each multicast group or range of groups allowed in the domain, excluding any group supported only by static RPs. The multicast groups allowed in the domain are determined by the aggregation of the groups allowed by the individually configured RPs and any static RPs. (Note that RP-Cs and static RP’s can be configured with overlapping support for a given set of multicast groups.)

Rendezvous-point tree (RPT)
When a DR in a VLAN receives traffic for a particular multicast group from a source on that VLAN, the DR encapsulates the traffic and forwards it to the RP elected to support that multicast group. The RP decapsulates the traffic and forwards it on toward the multicast receiver(s) requesting that group. This forms an RPT extending from the DR through any intermediate PIM-SM routers leading to the PIM-SM edge router(s) for the multicast receiver(s) requesting the traffic. (If the RP has no current join requests for the group, the traffic is dropped at the RP.)
Figure 19 Example PIM-SM domain with RPT active to support a host joining a multicast group

In default PIM-SM operation, the RPT path forms to deliver the first multicast packet from Group "X" to Host "Y". (Note that any router configured in the domain as a BSR candidate can be elected as the BSR.)

PIM-SM operation and router types 103

Shortest-path tree (SPT)

SPTs are especially useful in high data-rate applications where reducing unnecessary traffic concentrations and throughput delays are significant. In the default PIM-SM configuration, SPT operation is automatically enabled. (The software includes an option to disable SPT operation. See “Changing the shortest-path tree (SPT) operation” (page 83).)

Shortest-path tree operation

In the default PIM-SM configuration, after an edge router receives the first packet of traffic for a multicast group requested by a multicast receiver on that router, it uses Reverse Path Forwarding (RPF) to learn the shortest path to the group source. The edge router then stops using the RPT and begins using the shortest path tree (SPT) connecting the multicast source and the multicast receiver. In this case, when the edge router begins receiving group traffic from the multicast source through the SPT, it sends a prune message to the RP tree to terminate sending the requested group traffic on that route. (This results in entries for both the RP path and the STP in the routing table. See “Operating notes” (page 112).) When completed, the switchover from the RPT to a shorter SPT can reduce unnecessary traffic concentrations in the network and reduce multicast traffic throughput delays.

Note that the switchover from RPT to SPT is not instantaneous. For a short period, packets for a given multicast group may be received from both the RPT and the SPT. Also, in some topologies, the RPT and the SPT to the same edge router may be identical.
Restricting multicast traffic to RPTs

An alternate method to allowing the domain to use SPTs is to configure all of the routers in the domain to use only RPTs. However, doing so can increase the traffic load in the network and cause delays in packet delivery.

Maintaining an active route for multicast group members

The edge router itself and any intervening routers on the active tree between the members (receivers) of a multicast group and the DR for that group, send periodic joins. This keeps the active route available for as long as there is a multicast receiver requesting the group. When a route times out or is pruned, the DR ceases to send the requested group traffic on that route.

Border routers and multiple PIM-SM domains

Creating multiple domains enables a balancing of PIM-SM traffic within a network. Defining PIM-SM domain boundaries requires the use of PIM border routers (PMBRs), and multiple PMBRs can be used between any two domains.

**NOTE:** The software described in this guide does not support PMBR operation for PIM-SM networks.

**Pim-SM router types**

Within a PIM-SM domain, PIM-SM routers can be configured to fill one or more of the roles described in this section.

**DR:**

A router performing this function forwards multicast traffic from a unicast source to the appropriate distribution (rendezvous) point. See “DR” (page 105), below.

**BSR:**

A router elected to this function keeps all routers in a PIM-SM domain informed of the currently assigned RP for each multicast group currently known in the domain. See “BSR” (page 105).

**RP:**

A router elected as a RP for a multicast group receives requested multicast traffic from a DR and forwards it toward the multicast receiver(s) requesting the traffic. See “RP” (page 106).

**Static RP (static RP):**

This option forwards traffic in the same way as an RP, but requires manual configuration on all routers in the domain to be effective.
All of the above functions can be enabled on each of several routers in a PIM-SM domain.

**DR**

In a VLAN populated by one or more routers running PIM-SM, one such router is elected the DR for that VLAN. When the DR receives a Join request from a multicast receiver on that VLAN, it forwards the join toward the router operating as the RP for the requested multicast group.

Where multiple PIM-SM routers exist in a VLAN, the following criteria is used to elect a DR:
1. The router configured with the highest DR priority in the VLAN is elected.
2. If multiple routers in the VLAN are configured with the highest DR priority, the router having the highest IP address is elected.

In a given domain, each VLAN capable of receiving multicast traffic from a unicast source should have at least one DR. (Enabling PIM-SM on a VLAN automatically enables the router as a DR for that VLAN.) Because there is an election process for DR on each VLAN, all routers on a VLAN need to be enabled for DR. Where it is important to ensure that a particular router is elected as the DR for a given VLAN, you can increase the DR priority on that VLAN configuration for that router.

If it is necessary to prevent a router from operating as a DR on a given VLAN, disable DR operation by configuring the DR priority as zero (0).

**BSR**

Before a DR can forward encapsulated packets for a specific multicast group to an RP, it must know which router in the domain is the elected RP for that multicast group. The BSR function enables this operation by doing the following:
1. Learns the group-to-RP mappings on the C-RPs in the domain by reading the periodic advertisements each one sends to the BSR.
2. Distributes the aggregate C-RP information as an RP-set to the PIM-SM routers in the domain. This is followed by an election to assign a specific multicast group or range of groups to the C-RPs in the domain. (The software supports assignment of up to four multicast addresses and/or ranges of multicast addresses to a C-RP.)

The BSR periodically sends bootstrap messages to the other PIM-SM routers in the domain to maintain and update the RP-set data throughout the domain, and to maintain its status as the elected BSR.

**NOTE:** Where static RPs are configured in the domain to support the same multicast group(s) as one or more (dynamic) C-RPs, then the RP-set data has the precedence for assigning RPs for these groups unless the static RPs have been configured with the override option and if the multicast group mask for the static RP equals or exceeds the same mask for the applicable C-RP(s). See "NOTE" (page 108).

**BSR configuration and election**

There should be multiple BSR candidates configured in a PIM-SM domain so that if the elected BSR becomes unavailable, another router will take its place. In the BSR election process, the BSR candidate configured with the highest priority number is selected. Where the highest priority setting is shared by multiple candidates, the candidate having the highest IP address is selected. In the event that the selected BSR subsequently fails, another election takes place among the remaining BSR candidates. To facilitate a predictable BSR election, configure a higher priority on the router you want elected as the BSR for the domain. (See ???).

**NOTE:** A router serving as the BSR for a domain should be central to the network topology. This helps to ensure optimal performance and also reduce the possibility of a network problem isolating the BSR.
**BSR role in fault recovery**

If the hold-time maintained in the BSR for a given C-RP’s latest advertisement expires before being refreshed by a new advertisement from the C-RP, the non-reporting C-RP is removed from the domain. In this case, the removed C-RP’s multicast groups are re-assigned to other C-RPs. (If no other C-RPs or static RPs in the domain are configured to support a multicast group from the non-reporting C-RP, that group becomes unavailable in the domain.)

**RP**

Instead of flooding multicast traffic as is done with PIM-DM, PIM-SM uses a set of multiple routers to operate as RPs. Each RP controls multicast traffic forwarding for one or more multicast groups as follows:

- Receives traffic from multicast sources (S) via a DR.
- Receives multicast joins from routers requesting multicast traffic.
- Forwards the requested multicast traffic to the requesting routers.

Note that the routers requesting multicast traffic are either edge routers or intermediate routers. Edge routers are directly connected to specific multicast receivers using ICMP to request traffic. Intermediate routers are on the path between edge routers and the RP. This is known as a RP Tree (RPT) where only the multicast address appears in the routing table. For example:

\[( *, G ), \]

* = a variable (wildcard) representing the IP address of any multicast source
G = a particular multicast group address.

**NOTE:** The software supports up to 100 RPs in a given PIM-SM domain.

**Defining supported multicast groups**

An RP in the default candidate configuration supports the entire range of possible multicast groups. This range is expressed as a multicast address and mask, where the mask defines whether the address is for a single address or a range of contiguous addresses:

<table>
<thead>
<tr>
<th>Multicast address</th>
<th>Mask</th>
<th>Address range</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.0.0</td>
<td>240.0.0.0</td>
<td>224.0.0.0.0 - 239.255.255.255</td>
</tr>
</tbody>
</table>

An alternate way to express the above (default) address and mask is:

224.0.0.0/4

In non-default candidate configurations, an RP allows up to four ranges of contiguous multicast groups, and/or individual multicast groups, or both. For example:

<table>
<thead>
<tr>
<th>RP candidate configuration</th>
<th>Supported range of multicast groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>235.0.240.0/12</td>
<td>235.0.240.1 — 235.0.255.255</td>
</tr>
<tr>
<td>235.0.0.1/28</td>
<td>235.0.0.1 — 235.0.0.15</td>
</tr>
<tr>
<td>235.0.128/32</td>
<td>235.0.128 only</td>
</tr>
<tr>
<td>235.0.77/32</td>
<td>235.0.77 only</td>
</tr>
</tbody>
</table>

**NOTE:** If a given multicast group is excluded from all RPs in a given domain, then that group will not be available to the multicast receivers connected in the domain.

For more on this topic, see “Configuring C-RPs on PIM-SM routers” (page 79).
Within a PIM-SM domain, different RPs support different multicast addresses or ranges of multicast addresses. (That is, a given PIM-SM multicast group or range of groups is supported by only one active RP, although other C-RPs can also be configured with overlapping or identical support.)

A C-RP’s group-prefix configuration identifies the multicast groups the RP is enabled to support. If multiple C-RPs have group-prefixes configured so that any of these RPs can support a given multicast group, then the following criteria are used to select the RP to support the group:

1. The C-RP configured with the longest group-prefix mask applicable to the multicast group is selected to support the group. Step 2 of this procedure applies if multiple RP candidates meet this criterion.
2. The C-RP configured with the highest priority is selected. Step 3 of this procedure applies if multiple RP candidates meet this criterion.
3. A hash function (using the configured **bsr-candidate hash-mask-length** value) generates a series of mask length values that are individually assigned to the set of eligible C-RPs. If the hash function matches a single RP candidate to a longer mask length than the other candidates, that candidate is selected to support the group. Apply step 4 of this procedure if the hash function matches the longest mask length to multiple RP candidates.
4. The C-RP having the highest IP address is selected to support the group.

**NOTE:** In a PIM-SM domain where there are overlapping ranges of multicast groups configured on the C-RPs, discrete ranges of these groups are assigned to the domain’s C-RPs in blocks of sequential group numbers. The number of multicast groups in the blocks assigned within a given domain is determined by the **bsr-candidate hash-mask-length** value (range=1 to 32; See ??? configured on the elected BSR for the domain. A higher value means fewer sequential group numbers in each block of sequential group numbers, which results in a wider dispersal of multicast groups across the C-RPs in the domain.

As indicated above, multiple C-RPs can be configured to support the same multicast group(s). This is the generally recommended practice and results in redundancy that helps to prevent loss of support for desired multicast groups in the event that a router in the domain becomes unavailable. Configuring a C-RP to support a given multicast group does not ensure election of the C-RP to support that group unless the group is excluded from all other RPs in the domain. See .

Also, within a PIM-SM domain, a router can be configured as a C-RP available for a given multicast group or range of groups and as the static RP for a given multicast group or range of groups. The recommended practice is to use C-RPs for all multicast groups unless there is a need to ensure that a specific group or range of groups is always supported by the same routing switch. See “Static RP (static RP)” (page 107).

**Redundant Group Coverage Provides Fault-Tolerance**

If a C-RP elected to support a particular multicast group or range of groups becomes unavailable, the router is excluded from the RP-set. If the multicast group configuration of one or more other C-RPs overlaps the configuration in the failed RP, then another C-RP is elected to support the multicast group(s) formerly relying on the failed RP.

**Static RP (static RP)**

**General application**

Like C-RPs, static RPs control multicast forwarding of specific multicast groups or ranges of contiguous groups. However, static RPs are not dynamically learned, and increase the configuration and
monitoring effort needed to maintain them. As a result, static RPs are not generally recommended for use except where one of the following conditions applies:

- It is desirable to designate a specific router interface as a backup RP for specific group(s).
- Specific multicast groups are expected, and a static RP would help to avoid overloading a given RP with a high volume of multicast traffic.
- A C-RP for the same group(s) is less reliable than another RP that would not normally be elected to support the group(s).
- Tighter traffic control or a higher priority is desired for specific multicast groups.

**NOTE:** While the use of C-RPs and a BSR enable a dynamic selection of RPs for the multicast group traffic in a network, using static RPs involves manually configuring all routers in the domain to be aware of each static RP. This can increase the possibility of multicast traffic failure from misconfigurations within the PIM-SM domain. Also, because a BSR does not administer static RPs, troubleshooting PIM-SM traffic problems can become more complex. For these reasons, use of static RPs should be limited to applications where no viable alternatives exist, or where the network is stable and requires configuring and maintaining only a few routers.

If a static RP operating as the primary RP for a multicast group fails, and the PIM-SM configuration in the domain does not include a (secondary) dynamic RP (C-RP) backup to the static RP, then new multicast groups assigned to the static RP will not be available to multicast receivers in the domain. Also, if a static RP fails, support for existing groups routed through SPTs that exclude the failed router will continue, but any existing flows routed through the RPT will fail.

### Supporting a static RP as primary

A static RP can be configured to operate as either a secondary or primary RP. With the primary option, a dynamic (C-RP) backup is recommended. The precedence of a static RP over a dynamic RP is determined by the following static RP configuration options:

- override enabled on the static RP.
- A group mask on the static RP that equals or exceeds the group mask on the C-RP for the same multicast group(s).

For override configuration information, see “Statically configuring an RP to accept multicast traffic” (page 83).

### Operating rules for static RPs

- Static RPs can be configured on the same routers as C-RPs.
- Where a C-RP and a static RP are configured to support the same multicast group(s), the C-RP takes precedence over the static RP unless the static RP is configured to override the C-RP. (See “Supporting a static RP as primary” (page 108).)
- Any static RP in a domain must be configured identically on all routers in the domain. Otherwise, some DRS will not know of the static RP and will not forward the appropriate multicast traffic, and some routers will not know where to send Joins for the groups supported by static RP.
- Up to four static RP entries can be configured on a router. Each entry can be for either a single multicast group or a range of contiguous groups.
- Only one interface can be configured as the static RP for a given multicast group or range of groups. For example, a properly configured PIM-SM domain does not support configuring 10.10.10.1 and 10.20.10.1 to both support a multicast group identified as 239.255.255.10.
Static RPs are not included in the RP-set messages generated by the BSR, and do not generate advertisements.

If a static RP becomes unavailable, it is necessary to remove and/or replace the configuration for this RP in all routers in the domain.

**Configuration**

See “Statically configuring an RP to accept multicast traffic” (page 83).

**Operating rules and recommendations**

**Guideline for configuring C-RPs and BSRs**

Routers in a PIM-SM domain should usually be configured as both C-RPs and candidate BSRs; this can reduce some overhead traffic.

The SPT policy should be the same for all RPs in a domain.

Allowing some RPs to remain configured to implement SPTs while configuring other RPs in the same domain to force RPT use can result in unstable traffic flows. (Use the `[no] ip pim-sparse spt-threshold` command to change between SPT and RPT operation on each router.)

**Application of RPs to multicast groups.**

In a PIM-SM domain, a given multicast group or range of groups can be supported by only one RP. (Typically, multiple C-RPs in a domain are configured with overlapping coverage of multicast groups, but only one such candidate will be elected to support a given group.)

Ensuring that the C-RPs in a PIM-SM domain cover all desired multicast groups.

All of the multicast groups you want to allow in a given PIM-SM domain must be included in the aggregate of the multicast groups configured in the domain’s C-RPs. In most cases, all C-RPs in a domain should be configured to support all RP groups (the default configuration for a router enabled as a C-RP). This provides redundancy in case an RP becomes unavailable. (If the C-RP supporting a particular multicast group becomes unavailable, another C-RP is elected to support the group as long as there is redundancy in the C-RP configuration for multiple routers.) Note that is cases where routers are statically configured to support a specific group or range of groups, the C-RP prioritization mechanism allows for redundant support.

**PIM-SM and PIM-DM.**

These two features cannot both be enabled on the same router at the same time.

**Supporting PIM-SM across a PIM Domain.**

To properly move multicast traffic across a PIM-SM domain, all routers in the domain must be configured to support PIM-SM. That is, a router without PIM-SM capability blocks routed multicast traffic in a PIM-SM domain.

**Configuration steps for PIM-SM**

This process assumes that the necessary VLANs and IP addressing have already been configured on the routing switch.

**NOTE:** The switches described in this guide do not support PMBR operation in the current software release.

**Planning considerations**

- Where multiple routers are available to operate as the DR for a given source, set the DR priority on each router according to how you want the router used.
- Determine whether there are any bandwidth considerations that would call for disabling SPT operation. (If any routers in the domain have SPT operation disabled, it should be disabled on all RPs in the domain. See “Operating rules for static RPs” (page 108).)
• Determine the routers to configure as C-BSRs. In many applications, the best choice may be to configure all routers in the domain as candidates for this function.
• Determine the multicast group support you want on each C-RP and any static RPs in the domain. The easiest option is to enable C-RP to support all possible multicast groups on all routers in the domain. However, if there are traffic control considerations you want to apply, you can limit specific multicast groups to specific routers and/or set priorities so that default traffic routes support optimum bandwidth usage.

**Per-router global configuration context**

Use these steps to enable routing and PIM operation in the global configuration context of each PIM-SM router (HP(config)#):

1. Enable routing. (Use ip routing.)
2. Enable multicast routing. (Use ip multicast-routing.)
3. Enable PIM. (Use router pim.)
4. Configure the routing method(s) needed to reach the interfaces (VLANs) on which you want multicast traffic available for multicast receivers in your network:
   - Enable RIP or OSPF. (Use routerrip|ospf)
   - If desired, configure static routes to the destination subnets. (Use ip route dest-ip-address/mask-bits next-hop-ip-addr.)

**Per-VLAN PIM-SM configuration**

These steps configure PIM-SM in the VLAN interface context for each VLAN configured on the router (HP Switch(vlan-vid)#).

1. Enable IGMP. (Use ip igmp.) Repeat this action on every router (and switch) having membership in the VLAN.
2. For both the global and VLAN levels on the routers where there are connected multicast receivers that may issue joins or send multicast traffic, use the same routing method as Step 4 of this procedure.
3. Enable PIM-SM on the VLAN interfaces where you want to allow routed multicast traffic. (Default: disabled)
   a. If these VLANs do not already have static IP addresses, then statically configure one or more IP addresses on each VLAN you want to support PIM-SM operation. (PIM-SM cannot be enabled on a VLAN that does not have a statically configured IP address. That is, PIM-SM cannot use an IP address acquired by DHCP/Bootp.)
   b. Use ip pim-sparse to enter the VLAN’s pim-sparse context and do one of the following:
      • Enable PIM-SM on the VLAN and allow the default option (any) to dynamically determine the source IP address for the PIM-SM packets sent from this VLAN interface.
      • Enable PIM-SM on the VLAN and allow the default option (any) to dynamically determine the source IP address for the PIM-SM packets sent from this VLAN interface.
      • Enable PIM-SM on the VLAN and specify an IP address for the PIM-SM packets sent from this VLAN interface. (The specified IP address must already be statically configured on the VLAN.)
NOTE: This step requires enabling Router PIM on the global configuration context. See “Configuring global context commands” (page 71).

c. **Option**: Change the current DR priority, in the PIM Sparse context, to a value for the current router in the current VLAN by using Command dr-priority [0-4294967295].
(DR Priority default = 1)

**NOTE**: When you initially enable PIM-SM, it is recommended that you leave the PIM-SM traffic control settings at their default settings. You can then assess performance and make configuration changes where a need appears.

4. **Option**: Change one or more of the traffic control settings for the pim-sparse of a given VLAN on which PIM-SM is enabled. (Note that some VLAN context control settings apply to both PIM-SM and PIM-DM.) See “NOTE” (page 111)??

<table>
<thead>
<tr>
<th>Features accessed in VLAN-vid-pim-sparse context</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-addr(page 74)</td>
<td>Sets or resets the source IP address for PIM-SM packets sent out on the interface. Also enables PIM-SM on the interface. (Default: any)</td>
</tr>
<tr>
<td>hello-interval(^1)(page 74)</td>
<td>Resets the interval between transmitted PIM Hello packets on the interface. (Default: 30 seconds)</td>
</tr>
<tr>
<td>hello-delay(^1)(page 75)</td>
<td>Resets the maximum delay for transmitting a triggered PIM Hello packet on the interface. (Default: 5 seconds)</td>
</tr>
<tr>
<td>lan-prune-delay(^1)(page 75)</td>
<td>Enables or disables the LAN prune delay feature on the interface. (Default: on)</td>
</tr>
<tr>
<td>override-interval(^1)(page 76)</td>
<td>Resets the override interval of the LAN prune delay configured on the interface. (Default: 2500 milliseconds)</td>
</tr>
<tr>
<td>propagation-delay(^1)(page 76)</td>
<td>Resets the delay interval for triggering LAN prune delay packets on the interface. (Default: 500 milliseconds)</td>
</tr>
</tbody>
</table>
| dr-priority\(^1\)(page 76)                       | Resets the priority of the interface in the Designated Router election process. (Default: 1)
If you want one router on a given VLAN to have a higher priority for DR than other routers on the same VLAN, use the dr-priority command to reconfigure the DR priority setting as needed. Otherwise, the highest DR priority among multiple routers on the same VLAN interface is assigned to the router having the highest source IP address for PIM-SM packets on that interface. |

\(^1\) Applies to both PIM-SM and PIM-DM operations.

**Router Pim configuration**

These Steps configure the PIM-SM in the Router PIM context (HP Switch (pim)#).

1. **Specify the VLAN interface to advertise as the BSR Candidate and enable the router to advertise itself as a candidate BSR in a PIM-SM domain. (Use bsr-candidate source-ip-vlan vid.)**

2. **Option**: To make NSR candidate selection occur quickly and predictably, set a different priority on each BSR candidate in the domain. (Use bsr-candidate priority.)
3. Do one of the following to configure RP operation:
   - **Recommended:** Enable C-RP operation and configure the router to advertise itself as a C-RP to the BSR for the current domain. This step includes the option to allow the C-RP to be a candidate for either all possible multicast groups or for up to four multicast groups and/or ranges of groups. (Use `rp-candidate source-ip-vlan vid [group-addr/group-mask].`)
   - **Option:** Use `rp-address ip-addr [group-addr/group-mask]` to statically configure the router as the RP for a specific multicast group or range of multicast groups. (This must be configured on all RIM-SM routers in the domain.)

4. **Option:** In the PIM router context, change one or more of the traffic control settings. See Table 10 (page 112).

### Table 10 Options Accessed in Router PIM Context

<table>
<thead>
<tr>
<th>Options Accessed in Router PIM Context</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp-candidate group-prefix</td>
<td>Enter an address and mask to define an additional multicast group or a range of groups.</td>
</tr>
<tr>
<td>group-addr/group-mask</td>
<td></td>
</tr>
<tr>
<td>rp-candidate hold-time 30-255</td>
<td>Tells the BSR how long it should expect the sending C-RP router to be operative. (Default: 150; 0 if router is not a candidate.)</td>
</tr>
<tr>
<td>rp-candidate priority 0-255</td>
<td>Changes the priority for the C-RP router. When multiple C-RPs are configured for the same multicast group(s), the priority determines which router becomes the RP for such groups. A smaller value means a higher priority. (Default: 192)</td>
</tr>
<tr>
<td>[ no ] spt-threshold</td>
<td>Disable or enable the router’s ability to switch multicast traffic flows to the shortest path tree. (Default: enabled)</td>
</tr>
<tr>
<td>join-prune-interval 5-65535</td>
<td>Option: Globally change the interval for the frequency at which join and prune messages are forwarded on the router’s VLAN interfaces. (Default: 60 seconds)</td>
</tr>
<tr>
<td>trap neighbor-loss</td>
<td>hardware-mrt-full</td>
</tr>
</tbody>
</table>

**Operating notes**

**Eliminating redundancy in support for a multicast group**

Configuring only one router in a domain as an RP for supporting traffic for a specific multicast group eliminates support redundancy for that group. In this case, if that router becomes unavailable, the group will be excluded from the domain.

**Excluding multicast groups**

If all of the C-RPs and static RPs (if any) in a domain are configured to exclude some multicast groups or ranges of groups, multicast traffic for such groups will be dropped when received by a DR, and will not be forwarded to any RP. (Such groups will still be switched locally if IGMP is enabled on the VLAN where the excluded group traffic is received from a multicast traffic source.)

**Routing table entries**

For multicast traffic from a source to the edge router supporting a multicast receiver requesting the traffic, when an SPT forms, the routing table (on the edge router) will contain both of the following for the supported group:

- (S,G) entry for the source IP address and IP multicast group address supported by the SPT.
- (*,G) entry for the "any" (wildcard) source and (same) multicast group supported by the RP tree.
Flow capacity

The router supports up to 2048 flows. A router acting as a DR or RP has a significantly higher CPU load than other routers in a PIM-SM domain.

IP addresses acquired through DHCP

PIM-SM operation requires statically configured IP addresses and does not operate with IP addresses acquired from a DHCP server.

Event log messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast-addr / mask</td>
<td>Inconsistent address and mask. The mask entered for the specified multicast address does not specify sufficient bits to include the nonzero bits in the mask.</td>
</tr>
<tr>
<td>pkt-type pkt, src IP [ip-addr] vid [vid-#] (not a nbr)</td>
<td>A PIM packet was received that does not have a neighbor.</td>
</tr>
<tr>
<td>Bad parameter-name in pkt-type pkt from IP ip-addr</td>
<td>The PIM packet was dropped because of a bad parameter in the packet from the IP address shown.</td>
</tr>
<tr>
<td>BSM send to ip-addr failed</td>
<td>A BSM send failed. The IP address shown is the BSM destination address.</td>
</tr>
<tr>
<td>Candidate BSR functionality disabled pkt-type</td>
<td>Candidate BSR functionality has been disabled.</td>
</tr>
<tr>
<td>C-RP functionality disabled pkt-type</td>
<td>C-RP functionality has been disabled.</td>
</tr>
<tr>
<td>C-RP advertisement send to ip-addr failed</td>
<td>A C-RP advertisement send failed. The IP address shown is the destination address of the message.</td>
</tr>
<tr>
<td>Enabled as Candidate BSR using address: ip-addr</td>
<td>Candidate BSR functionality has been enabled at the indicated IP address.</td>
</tr>
<tr>
<td>Enabled as C-RP using address: ip-addr</td>
<td>C-RP functionality has been enabled at the indicated IP address.</td>
</tr>
<tr>
<td>Failed alloc of HW flow for flow src-ip-addr, multicast-addr</td>
<td>Hardware resources are consumed and software routing is being done for the flow.</td>
</tr>
<tr>
<td>Failed to initialize pkt-type as a call back routine</td>
<td>The IP address manager PIM callback routine failed to initialize.</td>
</tr>
<tr>
<td>Failed to alloc a pkt-type pkt (vid vid-#)</td>
<td>Allocation of a packet buffer failed message.</td>
</tr>
<tr>
<td>I/F configured with IP ip-addr on vid vid-#</td>
<td>The IP address on the PIM interface has changed to the indicated address.</td>
</tr>
<tr>
<td>I/F removal with IP ip-addr on vid vid-#</td>
<td>The PIM interface has been removed because of IP address removal or change of the indicated IP address.</td>
</tr>
<tr>
<td>Illegal operation in BSR state machine</td>
<td>An illegal state/event combination has been detected in the BSR state machine.</td>
</tr>
<tr>
<td>Malformed C-RP adv recvd from ip-addr</td>
<td>The switch received a malformed C-RP advertisement.</td>
</tr>
<tr>
<td>MCAST MAC add for mac-addr failed</td>
<td>The indicated interface could not join the multicast group for PIM packets.</td>
</tr>
<tr>
<td>Message</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>MCAST flow src-ip-addr, multicast-addr not rteing (rsc low)</td>
<td>A multicast flow has been dropped due to low resources</td>
</tr>
<tr>
<td>Multicast Hardware Failed to initialize</td>
<td>The multicast hardware cannot be enabled.</td>
</tr>
<tr>
<td>No IP address configured on VID vid-#</td>
<td>An IP address is not configured for the indicated interface enabled with PIM.</td>
</tr>
<tr>
<td>No route to source/rp ip-addr</td>
<td>PIM was unable to find a route to the specified IP address.</td>
</tr>
<tr>
<td>No RP for group ip-addr</td>
<td>PIM-SM needed an RP for the indicated group address, but none was found.</td>
</tr>
<tr>
<td>Inconsistent address and mask</td>
<td>The group prefix needs a route/mask entry. For example, if you want, 224.x.x.x/4, you input 224.0.0.0/4.</td>
</tr>
<tr>
<td>Pkt dropped from ip-addr reason, vid vid-#</td>
<td>Received a packet from the indicated IP address and VLAN, and dropped it.</td>
</tr>
<tr>
<td>Pkt rcvd with a cksum error from ip-addr</td>
<td>A packet arrived from the indicated IP address with a checksum error.</td>
</tr>
<tr>
<td>PIM socket error</td>
<td>There was an error regarding the PIM socket, either on a sockopt call or a recvfrom call.</td>
</tr>
<tr>
<td>Rcvd pkt ver# #, from ip-addr, expected #</td>
<td>Received a packet from the indicated IP address with the wrong PIM version number.</td>
</tr>
<tr>
<td>Rcvd pkt from rtr ip-addr, unkwn pkt type pkt-type</td>
<td>Unknown PIM packet type received from the indicated IP address.</td>
</tr>
<tr>
<td>Rcvd hello from ip-addr on vid vid-#</td>
<td>A misconfiguration exists between the routers.</td>
</tr>
<tr>
<td>Rcvd incorrect hello from ip-addr</td>
<td>An incorrect hello packet was received from the indicated IP address.</td>
</tr>
<tr>
<td>Rcvd unkwn opt # in pkt-type pkt from ip-addr</td>
<td>A PIM packet with an unknown option number was received from the indicated IP address.</td>
</tr>
<tr>
<td>Rcvd unkwn addr fmlly add-family in pkt-type pkt from ip-addr</td>
<td>A PIM packet with an unknown address family was received.</td>
</tr>
<tr>
<td>Rcvd pkt-type pkt with bad len from ip-addr</td>
<td>A PIM packet with an inconsistent length was received from the indicated IP address.</td>
</tr>
<tr>
<td>Send error( error-# ) on packet-type pkt on VID vid-#</td>
<td>Send packet failed on the indicated VLAN.</td>
</tr>
<tr>
<td>Static RP configuration failure: src-ip-addr, multicast-addr</td>
<td>The configuration of a static RP for the indicated multicast group has failed on the indicated interface.</td>
</tr>
<tr>
<td>Unable to alloc a buf of size size for memory element</td>
<td>PIM_DM could not allocate memory for the indicated buffer.</td>
</tr>
<tr>
<td>Unable to alloc a msg buffer for system-event</td>
<td>Informs the user that a message buffer could not be allocated for the indicated system event.</td>
</tr>
<tr>
<td>Unable to allocate table-type table</td>
<td>The PIM interface has been removed due to an IP address removal or change.</td>
</tr>
<tr>
<td>Message</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Unexpected state/event state /event in statemachine statemach</td>
<td>PIM received an event type in a state that was not expected.</td>
</tr>
<tr>
<td>VLAN is not configured for IP.</td>
<td>A VLAN must be statically configured with a primary IP address before enabling PIM-SM on that VLAN. If the VLAN has no IP address or is configured to acquire a primary IP address by using DHCP/Bootp, it cannot be configured to support PIM-SM.</td>
</tr>
</tbody>
</table>
## 4 Routing Basics

### Table 11 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip route</td>
<td>Displays the IP route table.</td>
<td>-</td>
<td>(page 116)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip arp-age [1...1440</td>
<td>infinite]</td>
<td>20 minutes</td>
<td>(page 116)</td>
<td>(page 117)</td>
</tr>
<tr>
<td></td>
<td>Allows the ARP age to be set from 1 to 1440 minutes (24 hours).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip router-id ip-addr</td>
<td>Changes the router ID.</td>
<td>-</td>
<td>(page 118)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip proxy-arp</td>
<td>Disables IP proxy ARP.</td>
<td>-</td>
<td>(page 118)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip local-proxy-arp</td>
<td>Enables the local proxy ARP option.</td>
<td>Disabled</td>
<td>(page 118)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip directed-broadcast</td>
<td>Enables forwarding of IP directed broadcasts</td>
<td>Disabled</td>
<td>(page 119)</td>
<td></td>
</tr>
<tr>
<td>[no] ip icmp echo broadcast-request</td>
<td>Disables response to ping requests on a global basis.</td>
<td>Enabled</td>
<td>(page 120)</td>
<td></td>
</tr>
<tr>
<td>[no] ip icmp unreachable</td>
<td>Disables all ICMP unreachable messages.</td>
<td>-</td>
<td>(page 120)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip icmp redirects</td>
<td>Disables ICMP redirects on the HP routing switch on a global basis, for all the routing-switch interfaces</td>
<td>-</td>
<td>(page 120)</td>
<td>-</td>
</tr>
</tbody>
</table>

For an overview of IP routing, see “Overview of IP routing” (page 120).

### Viewing the IP route table

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>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1/32</td>
<td>10.10.12.1</td>
<td>connected</td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

### Increasing ARP age timeout (CLI)

The address resolution protocol (ARP) age is the amount of time the switch keeps a MAC address learned through ARP in the ARP cache. The switch resets the timer to zero each time the ARP entry is refreshed and removes the entry if the timer reaches the ARP age. For more information on ARP, see “IP tables and caches” (page 121).

**Syntax:**

```
[no] ip arp-age [1...1440] | infinite ]
```

Allows the ARP age to be set from 1 to 1440 minutes (24 hours).

If the option `infinite` is configured, the internal ARP age timeout is set to 99,999,999 seconds (approximately 3.2 years). An `arp-age` value of 0 (zero) is stored in the configuration file to indicate that `infinite` has been configured. This value also displays with the `show` commands and in the menu display (Menu Switch Configuration IP Config).
Default: 20 minutes

Example

Example 57 Setting the ARP age timeout to 1000 minutes

HP Switch(config)# ip arp-age 1000

Example 58 Show IP command displaying ARP age

To view the value of ARP age timer, enter the `show ip` command. The Arp Age time value is shown in bold below.

HP Switch(config)# show ip
Internet (IP) Service
IP Routing : Disabled
Default Gateway : 15.255.120.1
Default TTL : 64
Arp Age : 1000
Domain Suffix : DNS server :
VLAN | IP Config | IP Address | Subnet Mask | Proxy ARP
--- | ---------- | ----------- | ------------ | -------
DEFAULT_VLAN | Manual | 15.255.111.13 | 255.255.248.0 | No

Example 59 IP ARP-age value in the running config file

You can also view the value of the ARP age timer in the configuration file. The `ip arp-age 1000` value is shown in bold below.

HP Switch(config)# show running-config
Running configuration:
; J9091A Configuration Editor; Created on release #K.15.XX
hostname "8200LP"
module 2 type J8702A
module 3 type J8702A
module 4 type J8702A
ip default-gateway 15.255.120.1
ip arp-age 1000
snmp-server community "public" Unrestricted
snmp-server host 16.180.1.240 "public"
vlan 1
    name "DEFAULT_VLAN"
    untagged B1-B24,C1-C24,D1-D24
    ip address 15.255.120.85 255.255.248.0
exit
gvrp
spanning-tree

Setting and viewing the arp-age value (Menu)

You can set or display using the menu interface (`Menu Switch Configuration IP Config`).
If you want to change the router ID setting, do the following:

1. Go to the global config context; the CLI prompt appears similar to the following:
   
   `HP Switch(config)#`

2. If OSPF is not enabled, go to step 3 (page 118); if OSPF is enabled, use `no router ospf` to disable OSPF operation.

3. Use `ip router-id ip-addr` to specify a new router ID. (This IP address must be unique in the routing switch configuration.)

4. If you disabled OSPF operation in step 2 (page 118), use `router ospf` to re-enable OSPF operation.

For more information on the router ID, see “IP global parameters for routing switches” (page 123) and “Changing the router ID” (page 126).

### Changing the router ID

`HP Switch(config)# ip router-id 209.157.22.26`

**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.

### Enabling proxy ARP

Proxy ARP is disabled by default on HP routing switches. Enter the following commands from the VLAN context level in the CLI to enable proxy ARP:

`HP Switch(config)# vlan 1`

`HP Switch(vlan-1)# ip proxy-arp`

To again disable IP proxy ARP, enter:
Enabling local proxy ARP

When the local proxy ARP option is enabled, a switch responds with its MAC address to all ARP request on the VLAN. All IP packets are routed through and forwarded by the switch. The switch prevents broadcast ARP requests from reaching other ports on the VLAN.

**NOTE:** Internet control message protocol (ICMP) redirects are disabled on interfaces on which local proxy ARP is enabled.

To enable local proxy ARP, you must first enter VLAN context, for example:

```
HP Switch(config) vlan 1
```

Then enter the command to enable local proxy ARP:

```
HP Switch(vlan-1)ip local-proxy-arp
```

**Syntax:**

```
[no] ip local-proxy-arp
```

Enables the local proxy ARP option. You must be in VLAN context to execute this command.

When enabled on a VLAN, the switch responds to all ARP requests received on the VLAN ports with its own hardware address.

The `no` option disables the local proxy ARP option.

Default: Disabled

Execute the `show ip` command to see which VLANs have local proxy ARP enabled.

**Example 6 1 Local proxy ARP is enabled on the default VLAN**

```
HP Switch(vlan-1)# show ip

Internet (IP) Service

IP Routing : Disabled

Default TTL : 64
Arp Age : 20
Domain Suffix :
DNS server :

| VLAN              | IP Config | IP Address      | Subnet Mask     | Proxy ARP |
|-------------------+-----------+-----------------+-----------------+-----------|
| DEFAULT_VLAN      | DHCP/Bootp | 15.255.157.54   | 255.255.248.0   | Yes Yes   |
| VLAN2100          | Disabled  |
```

Enabling forwarding of IP directed broadcasts (CLI)

For more information, see “Configuring forwarding parameters” (page 129).

```
HP Switch(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.

Disabling the directed broadcasts

```
HP Switch(config)# no ip directed-broadcast
```

Disabling replies to broadcast ping requests

By default, HP devices are enabled to respond to broadcast ICMP echo packets, which are ping requests (for more information, see “Disabling ICMP messages” (page 129). You can disable response to ping requests on a global basis using the following CLI command:

```
HP Switch(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:

```
HP Switch(config)# ip icmp echo broadcast-request
```

Disabling all ICMP unreachable messages

For more information, see “Disabling ICMP destination unreachable messages” (page 130).

```
HP Switch(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.

Enter the following command at the global CONFIG level of the CLI:

```
HP Switch(config)# no ip icmp redirects
```

Syntax:

```
[no] ip icmp redirects
```

Overview of IP routing

The switches offer the following IP routing features:

- Static routes
  - 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

License requirements:
In the 3500, 3500yl, 5400zl, 6600, and 8200zl switches, OSPF is included with the Premium License. In the 6200yl switches, this feature is included with the base feature set.

Throughout this chapter, the switches are 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 RIP.

For configuring the IP addresses, see chapter "Configuring IP Addresses" in the Management and Configuration Guide for your switch. Use the information in this chapter if you need to change some of the IP parameters from their default values or if 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 subnet. You can have only one VLAN interface in a given subnet. 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 32.
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 devices support configuration and display of IP address in classical subnet 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 subnet format only.

IP tables and caches
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 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:

**Example 62 ARP cache dynamic entry**

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>207.95.6.102</td>
<td>0800.5afc.ea21</td>
<td>Dynamic</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” (page 127).

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.

Routing paths

The IP route table can receive the routing paths from the following sources:

- Directly-connected destination, which means there are no router hops to the destination
- Static route, which is a user-configured route
- Route learned through RIP
- Route learned through OSPF

Administrative distance

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 to 255.

The IP route table is displayed by entering the `show ip route` command from any context level in the console CLI. Here is an example of an entry in the IP route table:

**Example 63 IP route table entry**

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Di</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1/32</td>
<td>10.10.12.1</td>
<td>connected</td>
<td></td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

Each IP route table entry contains the destination's IP address and subnet 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 subtype, and the route's IP metric (cost). The type indicates how the IP route table received the route.

Enter the `show ip route summary` command to display the aggregate count of routes for each routing protocol.
Example 64 IP route summary display

HP Switch(config)# show ip route summary

IPv4 Route Table Summary

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Active Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected</td>
<td>1</td>
</tr>
<tr>
<td>Static</td>
<td>1</td>
</tr>
</tbody>
</table>

To configure a static IP route, see “Static Routing” (page 131).

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 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. The age interval depends on the number of entries in the table. The age timer ranges from 12 seconds (full table) to 36 seconds (empty table). Entries are aged only if they are not being used by traffic. If you have an entry that is always being used in hardware, it will never age. If there is no traffic, it will age in 12 to 36 seconds. The age timer is not configurable.

**NOTE:** You cannot add static entries to the IP forwarding cache.

IP route exchange protocols

The switch supports the following IP route exchange protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- ICMP Router Discovery Protocol (IRDP)
- Dynamic Host Configuration Protocol (DHCP) Relay

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 parameters” (page 136)
- “Configuring OSPF on the routing switch” (page 152)
- “Configuring IRDP” (page 237)
- “Dynamic Host Configuration Protocol” (page 240)

IP global parameters for routing switches

Table 12 (page 124) lists the IP global parameters and the page where you can find more information about each parameter.
Table 12 IP global 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>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>126</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP)</td>
<td>A standard IP mechanism that routers use to learn the 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>127</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. (Can be set using the menu interface to be as long as 1440 minutes. Go to Menu Switch Configuration IP Config.) See “Increasing ARP age timeout (CLI)” (page 116).</td>
<td>Five minutes.</td>
<td>N/A</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>128</td>
</tr>
<tr>
<td>Time to Live (TTL)</td>
<td>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.</td>
<td>64 hops</td>
<td>See chapter “Configuring IP Addressing” in the Management and Configuration Guide.</td>
</tr>
<tr>
<td>Directed broadcast forwarding</td>
<td>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.</td>
<td>Disabled</td>
<td>(page 129)</td>
</tr>
</tbody>
</table>
### Table 12 IP global parameters for routing switches (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NOTE:</strong></td>
<td>You also can enable or disable this parameter on an individual interface basis. See Table 13 (page 125).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 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. | Disabled | A-21 A-159 |
| Forwarding method | (broadcast or multicast) | | |
| Hold time | | | |
| Maximum advertisement interval | | | |
| Minimum advertisement interval | | | |
| Router preference level | | | |

| Static route | An IP route you place in the IP route table. | No entries | A-25 |

| Default network route | The router uses the default network route if the IP route table does not contain a route to the destination. 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 | A-30 |

### IP interface parameters for routing switches

Table 13 (page 125) lists the interface-level IP parameters for routing switches.

### Table 13 IP interface parameters — 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>1</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>A-33</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 and overridden for individual VLAN interfaces. Other parameters can be configured on individual VLAN interfaces.

**NOTE:** For IP configuration information when routing is not enabled, see chapter "Configuring IP Addressing" in the Management and Configuration Guide for your switch.

### Configuring IP addresses

You can configure IP addresses on the routing switch's VLAN interfaces. Configuring IP addresses is described in detail in chapter "Configuring IP Addressing" in the Management and Configuration Guide for your switch.

### 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 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:** RIP does not use the router ID.

If no router ID is configured, then, by default, the router ID on an HP routing switch is the first IP address that becomes physically active at reboot. This is usually the lowest numbered IP interface configured on the device. However, if no router ID is configured, and one or more user-configured loopback interfaces are detected at reboot, the lowest-numbered (user-configured) loopback interface becomes the router ID. If the lowest-numbered loopback interface has multiple IP addresses, the lowest of these addresses will be selected as the router ID. Once a router ID is selected, it does not automatically change unless a higher-priority interface is configured on the routing switch and OSPF is restarted with a reboot. (User-configured loopback interfaces are always higher priority than other configured interfaces.) However, you can explicitly set the router ID to any valid IP address, as long as the IP address is not 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.

---

### Table 13 IP interface parameters — routing switches (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Router Discovery Protocol (IRDP)</td>
<td>Locally overrides the global IRDP settings. See Table 12 (page 124) for global IRDP information.</td>
<td>Disabled</td>
<td>A-159</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 subnet to a server on another subnet.</td>
<td>None configured</td>
<td>A-164</td>
</tr>
</tbody>
</table>

1 See chapter "Configuring IP Addressing" in the Management and Configuration Guide for your switch.
## Configuring ARP parameters

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

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Type</th>
<th>Default Cost</th>
<th>Stub</th>
<th>Summary LSA</th>
<th>Metric Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>backbone</td>
<td>normal</td>
<td>1</td>
<td>send</td>
<td>ospf metric</td>
<td></td>
</tr>
<tr>
<td>0.0.0.2</td>
<td>nssa</td>
<td>10</td>
<td>send</td>
<td>external type 2</td>
<td></td>
</tr>
<tr>
<td>0.0.0.3</td>
<td>stub</td>
<td>2</td>
<td>send</td>
<td>ospf metric</td>
<td></td>
</tr>
<tr>
<td>0.0.0.4</td>
<td>stub</td>
<td>10</td>
<td>send</td>
<td>ospf metric</td>
<td></td>
</tr>
</tbody>
</table>
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 of 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. For more information, see “About enabling proxy ARP” (page 128).

**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.

### About 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 subnets, 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 subnet cannot reach a device in the 20.20.20.0 subnet if the subnets are on different network cables, and thus is not answered.

An ARP request from one subnet can reach another subnet when both subnets are on the same physical segment (Ethernet cable), since MAC-layer broadcasts reach all the devices on the segment.

### Proxy ARP and local proxy ARP behavior

When local proxy ARP is enabled, all valid ARP requests receive a response.
When proxy ARP is enabled, all valid ARP requests receive a response if the following conditions are met:

- There is a route to the target IP address in the ARP request (this can be a route or default route), and the VLAN (interface) the ARP request is received on does NOT match the interface for the next hop in the matched route to get to the target IP address.

AND

- There is a route back to the source IP address in the ARP request and the interface the ARP request came in on DOES match the interface for the next hop in the matched route to get to the source IP address.

Configuring forwarding parameters

The following configurable parameters control the forwarding behavior of HP routing switches:

- Time-To-Live (TTL) threshold
  The configuration of this parameter is covered in the chapter "Configuring IP Addressing" in the Management and Configuration Guide for your routing switch.

- Forwarding of directed broadcasts
  These parameters are global and thus affect all IP interfaces configured on the routing switch.

Enabling forwarding of directed broadcasts

A directed broadcast is an IP broadcast to all devices within a single directly-attached network or subnet. A net-directed broadcast goes to all devices on a given network. A subnet-directed broadcast goes to all devices within a given subnet.

NOTE: A less common type, the all-subnets broadcast, goes to all directly-attached subnets. Forwarding for this broadcast type also is supported, but most networks use IP multicasting instead of all-subnet 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.

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 ICMP destination unreachable messages
By default, when a 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 subnet 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.
5 Static Routing

Table 14 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip route dest-ip-addr/mask-length [next-hop-ip-addr</td>
<td>vlan vlan-id</td>
<td>reject</td>
<td>blackhole</td>
<td>[metric metric] [distance 255] [tag-value tagval]`</td>
</tr>
<tr>
<td><code>show ip route static</code></td>
<td>Displays the current static route configuration on the routing switch.</td>
<td>-</td>
<td>(page 132)</td>
<td>-</td>
</tr>
</tbody>
</table>

This chapter describes how to add static and null routes to the IP route table. For more information, see the sections beginning with “Static route types” (page 133).

Configuring a static route

Static route
- Configure a static route to a specific network or host address

Null route
- Configure a "null" route to discard IP traffic to a specific network or host address:
  - Discard traffic for the destination, with ICMP notification to sender
  - Discard traffic for the destination, without ICMP notification to sender

Syntax:
```
[no] ip route dest-ip-addr / mask-length [next-hop-ip-addr | vlan vlan-id | reject | blackhole] [metric metric] [distance 255] [tag-value tagval]
```

Allows the addition and deletion of static routing table entries. A route entry is identified by a destination (IP address/mask length) and next-hop pair. The next-hop can be either a gateway IP address, a VLAN, or the keyword “reject" or “blackhole”. A gateway IP address does not have to be directly reachable on one of the local subnets. If the gateway address is not directly reachable, the route is added to the routing table as soon as a route to this address is learned.

```text
dest-ip-addr / mask-bits
The route destination and network mask length for the destination IP address. Alternatively, you can enter the mask itself.
For example, you can enter either 10.0.0.0/24 or 10.0.0.0 255.255.255.0 for a route destination of 10.0.0.0 255.255.255.0.

next-hop-ip-addr
This IP address is the gateway for reaching the destination. The next-hop IP address is not required to be directly reachable on a local subnet. (If the next-hop IP address is not directly reachable, the route will be added to the routing table as soon as a route to this address is learned.)

reject
Specifies a null route where IP traffic for the specified destination is discarded and an ICMP error notification is returned to the sender.
```
blackhole
Specifies a null route where IP traffic for the specified destination is discarded and no ICMP error notification is returned to the sender.

metric
Specifies an integer value that is associated with the route. It is used to compare a static route to routes in the IP route table from other sources to the same destination.

distance
Specifies the administrative distance to associate with a static route. If not specified, this value is set to a default of 1.
For more on this topic, See “Administrative distance” (page 122). (Range: 1 to 255)
tag
Specifies a unique integer value for a given ECMP set (destination, metric, distance).
The no form of the command deletes the specified route for the specified destination next-hop pair.

Example
The following example configures two static routes for traffic delivery and identifies two other null routes for which traffic should be discarded instead of forwarded.

Figure 22 Configuring static routes

```
HP Switch(config)# ip route 10.10.40.0/24 10.10.10.1
HP Switch(config)# ip route 10.10.50.128/27 10.10.10.1
HP Switch(config)# ip route 10.50.10.177/32 reject
HP Switch(config)# ip route 10.50.10.0/24 blackhole
```

Viewing static route information
The show ip route static command displays the current static route configuration on the routing switch. Example 65 (page 135) shows the configuration resulting from the static routes configured in the example above.
Figure 23 Displaying the currently configured static routes

```
HP Switch(config)# show ip route static
IP Route Entries
<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.50.10.177/32</td>
<td>reject</td>
<td>static</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.10.40.0/24</td>
<td>VLAN10</td>
<td>10</td>
<td>static</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.10.50.128/27</td>
<td>VLAN10</td>
<td>10</td>
<td>static</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.50.10.0/24</td>
<td>blackhole</td>
<td>static</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td>static</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.10.144.32/24</td>
<td>10.0.0.2</td>
<td>1</td>
<td>static</td>
<td>12</td>
<td>10</td>
</tr>
<tr>
<td>127.10.144.32/24</td>
<td>10.0.0.3</td>
<td>1</td>
<td>static</td>
<td>12</td>
<td>10</td>
</tr>
</tbody>
</table>
```

This reject (default null) route is included by default. Refer to “Configuring a static route” on page 1-1

An ECMP set with ip load-sharing set to 2 (the maximum paths allowed)

Configuring the default route

You can also assign the default route and enter it in the routing table. The default route is used for all traffic that has a destination network not reachable through any other IP routing table entry. For example, if 208.45.228.35 is the IP address of your ISP router, all non-local traffic could be directed to the ISP by entering this command:

```
HP Switch(config)# ip route 0.0.0.0/0 208.45.228.35
```

Static route types

You can configure the following types of static IP routes:

Standard

The static route consists of a destination network address or host, a corresponding network mask, and the IP address of the next-hop IP address.

Null (discard)

The null route consists of the destination network address or host, a corresponding network mask, and either the reject or blackhole keyword. Typically, the null route is configured as a backup route for discarding traffic if the primary route is unavailable. By default, when IP routing is enabled, a route for the 127.0.0.0/8 network is created to the null interface. Traffic to this interface is rejected (dropped).

This route is for all traffic to the "loopback" network, with the single exception of traffic to the host address of the switch’s loopback interface (127.0.0.1/32). Figure A-3 on page 1-6 shows the default null route entry in the switch’s routing table.

NOTE: On a single routing switch you can create one null route to a given destination. Multiple null routes to the same destination are not supported.

Other sources of routes in the routing table

The IP route table can also receive routes from the following sources:

- Directly connected networks: One route is created per IP interface. When you add an IP 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 RIP 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. See “Administrative distance” (page 122).
• OSPF: See RIP, but substitute "OSPF" for "RIP".
• Default 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” (page 133).

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 or host.
• The route’s path, which can be one of the following:
  • IP address of a next-hop router.
  • "Null" interface; the routing switch drops traffic forwarded to the null interface.

The routing switch also applies default values for the route’s administrative distance (page A-10). In the case of static routes, this is the value the routing switch uses to compare a static route to routes from other route sources to the same destination before placing a route in the IP route table. The default administrative distance for static IP routes is 1, but can be configured to any value from 1 to 255.

The fixed 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 VLAN states
IP static routes remain in the IP route table only so long as the IP interface to the next-hop router is up. If the next-hop interface goes down, the software removes the static route from the IP route table. If the next-hop interface comes up 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 unreachable paths, but instead uses routes only when their paths are reachable.

For example, the following command configures a static route to 207.95.7.0 (with a network mask of 255.255.255.0), using 207.95.6.157 as the next-hop router’s IP address.

```
HP Switch(config)# ip route 207.95.7.0/24 207.95.6.157
```

A static IP route specifies the route’s destination address and the next-hop router’s IP address or routing switch interface through which the routing switch can reach the destination. (The route is added to the routing switch’s IP route table.)

In the above example, routing switch "A" knows that 207.95.6.157 is reachable through port A2, and assumes that local interfaces within that subnet are on the same port. Routing switch "A" deduces that IP interface 207.95.7.188 is also on port A2. The software automatically removes a static route from the route table if the next-hop VLAN used by that route becomes unavailable. When the VLAN becomes available again, the software automatically re-adds the route to the route table.

Configuring equal cost multi-path (ECMP) routing for static IP routes
ECMP routing allows multiple entries for routes to the same destination. Each path has the same cost as the other paths, but a different next-hop router. The `ip load-sharing` command specifies the maximum number of equal paths that can be configured. Values range from 2 to 4. For more information about the `ip load-sharing` command, see page A-127.
Example 65 Example of an ECMP set with the same destination but different next-hop routers

This example shows configuration of an ECMP set with two different gateways to the same destination address but through different next-hop routers. For more information about ECMP, see “OSPF equal-cost multipath (ECMP) for different subnets available through the same next-hop routes” (page 213).

HP Switch(config)# ip route 127.10.144.21/24 10.10.10.2 metric 12 distance 10
HP Switch(config)# ip route 127.10.144.21/24 10.10.10.3 metric 12 distance 10
### 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-or-v2, if needed.

**Syntax:**

```
[no] router rip
```

To enable RIP on a routing switch, enter the following commands:

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] router rip</td>
<td>Enables RIP on a routing switch.</td>
<td>Disabled</td>
<td>(page 136)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router rip [enable]</td>
<td>Enables RIP on the routing switch and to enter the RIP router context.</td>
<td>Disabled</td>
<td>(page 137)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip rip [v1-only</td>
<td>v1-or-v2</td>
<td>v2-only]</td>
<td>Changes RIP type on a VLAN interface.</td>
<td>RIPv2-only</td>
</tr>
<tr>
<td>[no] ip rip [ip-addr] authentication-key key-string</td>
<td>Configures a RIP authentication key.</td>
<td></td>
<td>(page 138)</td>
<td>-</td>
</tr>
<tr>
<td>ip rip metric 1-16</td>
<td>Changes the cost increase that a VLAN interface adds to RIP routes learned on that interface.</td>
<td>1</td>
<td>(page 139)</td>
<td>-</td>
</tr>
<tr>
<td>restrict [ip-addr ip-mask</td>
<td>ip-addr /prefix length]</td>
<td>Prevents any routes with a destination address that is included in the range specified by the address/mask pair from being redistributed by RIP.</td>
<td></td>
<td>(page 139)</td>
</tr>
<tr>
<td>default-metric value</td>
<td>Changes the default metric.</td>
<td>1</td>
<td>(page 140)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router rip redistribute [connected</td>
<td>static</td>
<td>ospf] [route-map name]</td>
<td>Enables redistribution of the specified route type to the RIP domain.</td>
<td></td>
</tr>
<tr>
<td>[no] ip rip poison-reverse</td>
<td>Disables Poison reverse on an interface, thus enabling Split horizon.</td>
<td>Poison reverse</td>
<td>(page 141)</td>
<td>-</td>
</tr>
<tr>
<td>show ip rip</td>
<td>Displays general RIP information.</td>
<td>-</td>
<td>(page 141)</td>
<td>-</td>
</tr>
<tr>
<td>show ip rip interface [ip-addr</td>
<td>vlan vlan-id]</td>
<td>Displays RIP interface information.</td>
<td>-</td>
<td>(page 143)</td>
</tr>
</tbody>
</table>

To display RIP configuration information and statistics, see “Overview of RIP” (page 145). For more information on configuring RIP, see “Viewing RIP information” (page 141).
Enabling RIP on the routing switch and entering the RIP router context

Syntax:

```
[no] router rip [[enable] | [disable]] [auto-summary]
```

Executed at the global configuration level to enable RIP on the routing switch and to enter the RIP router context. This enables you to proceed with assigning RIP areas and to modify RIP global parameter settings as needed. Global IP routing must be enabled before the RIP protocol can be enabled.

- **enable**
  - Enables RIP routing.
- **disable**
  - Disables RIP routing.

Default: Disabled

The no form of the command deletes all protocol-specific information from the global context and interface context. All protocol parameters are set to default values.

**NOTE:** The no router rip command also disables RIP routing.

If you disable RIP, the switch retains all the configuration information for the disabled protocol in flash memory. If you subsequently restart RIP, the existing configuration will be applied.

The auto-summary form of the command enables advertisement of the summarized routes. When used with the no form of the command, auto-summary disables the advertisement of the summarized routes.
Example

Example 66 Enter RIP router context

HP Switch(config)# router rip
HP Switch(rip)#

Example 67 Enable RIP routing

HP Switch(config)# router rip enable
HP Switch(rip)#

Example 68 Disable RIP routing

HP Switch(config)# router rip disable
HP Switch(rip)#

Example 69 Delete all protocol-specific information from the global context and interface context and set all protocol parameters to default values

HP Switch(config)# no router rip
HP Switch(rip)#

Enabling IP RIP on a VLAN

To enable RIP on all IP addresses in a VLAN, use `ip rip` in the VLAN context. When the command is entered without specifying any IP address, it is enabled in all configured IP addresses of the VLAN.

To enable RIP on a specific IP address in a VLAN, use `ip rip [ip-addr | all]` in the VLAN context and enter a specific IP address. If you want RIP enabled on all IP addresses, you can specify all in the command instead of a specific IP address.

Configuring a RIP authentication key

Configures a RIP authentication key. There is a maximum of 16 characters.

Syntax:

```
[no] ip rip [ip-addr]
authentication-key key-string
```

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

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 - or - version 2

Syntax:

```
[no] ip rip [v1-only | v1-or-v2 | v2-only ]
```
To change the RIP type supported on a VLAN interface, enter commands such as the following:

```
HP Switch(config)# vlan 1
HP Switch(vlan-1)# ip rip v1-only
HP Switch(vlan-1)# exit
HP Switch(config)# write memory
```

### Changing the cost of routes learned on a VLAN interface

By default, the switch interface increases the cost of an 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 switch from using a specific interface for routes learned through that interface by setting its metric to 16.

**Syntax:**

```
ip rip metric 1-16
```

To increase the cost a VLAN interface adds to RIP routes learned on that interface, enter commands such as the following:

```
HP Switch(config)# vlan 1
HP Switch(vlan-1)# ip rip metric 5
```

These commands configure vlan-1 to add 5 to the cost of each route learned on the interface.

### Configuring for redistribution

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.

**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.

**NOTE:** Do not enable redistribution until you have configured the redistribution filters. Otherwise, the network might become overloaded with routes that you did not intend to redistribute.

**Example**

To configure the switch to filter out redistribution of static, connected, or OSPF routes on network 10.0.0.0, enter the following commands:

```
HP Switch(config)# router rip
HP Switch(rip)# restrict 10.0.0.0 255.0.0.0
HP Switch(rip)# write memory
```

**NOTE:** The default configuration permits redistribution for all default connected routes only.
Modifying 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 to 15.

Syntax:

```
default-metric value
```

The value can be from 1 to 15. The default is 1.

Example

To assign a default metric of 4 to all routes imported into RIP, enter the following commands:

```
HP Switch(config)# router rip
HP Switch(rip)# default-metric 4
```

Enabling RIP route redistribution

The basic form of the `redistribute` command redistributes all routes of the selected type. For finer control over route selection and modification of route properties, you can specify the `route-map` parameter and the name of a route map. (For general information on route policy and route maps, see “Route Policy” (page 215). For examples of using route maps in route redistribution, see “Using route policy in route redistribution” (page 225).)

**NOTE:** Do not enable redistribution until you have configured the redistribution filters. Otherwise, the network might become overloaded with routes that you did not intend to redistribute.

Syntax:

```
[no] router rip redistribute [ connected | static | ospf ]
[route-map name]
```

Enables redistribution of the specified route type to the RIP domain.

- **static**
  - Distribute from manually configured routes.

- **connected**
  - Distribute from locally connected networks.

- **ospf**
  - Distribute from OSPF routes.

```
route-map name
```

Optionally specify the name of a route-map to apply during redistribution. The `no` form of the command disables redistribution for the specified route type.

Example

To enable redistribution of all connected, static, and OSPF routes into RIP, enter the following commands.

```
HP Switch(config)# router rip
HP Switch(rip)# redistribute connected
HP Switch(rip)# redistribute static
HP Switch(rip)# redistribute ospf
HP Switch(rip)# write memory
```
Changing the route loop prevention method

For more information about Poison reverse and Split horizon, see “Changing the route loop prevention method” (page 148).

Syntax:

```
[no] ip rip poison-reverse
```

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:

```
HP Switch(config)# vlan 1
HP Switch(vlan-1)# no ip rip poison-reverse
```

Entering the command without the `no` option re-enables Poison reverse.

Viewing RIP information

All RIP configuration and status information is shown by the CLI command `show ip rip` and options off that command.

Viewing general RIP information

Syntax:

```
show ip rip
```

To display general RIP information, enter `show ip rip` at any context level. The resulting display will appear similar to the following:

**Example 70 General RIP information listing**

```
HP Switch(config)# show ip rip

RIP global parameters

<table>
<thead>
<tr>
<th>RIP protocol: enabled</th>
<th>Auto-summary: enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Metric: 4</td>
<td></td>
</tr>
<tr>
<td>Distance: 120</td>
<td></td>
</tr>
<tr>
<td>Route changes: 0</td>
<td></td>
</tr>
<tr>
<td>Queries: 0</td>
<td></td>
</tr>
</tbody>
</table>

RIP interface information

<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>5</td>
<td>none</td>
</tr>
<tr>
<td>100.2.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>5</td>
<td>none</td>
</tr>
<tr>
<td>100.3.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>5</td>
<td>none</td>
</tr>
<tr>
<td>100.4.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>5</td>
<td>none</td>
</tr>
</tbody>
</table>

RIP peer information

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Bad routes</th>
<th>Last update timeticks</th>
</tr>
</thead>
</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, 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 worst, 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
      Address of the VLAN interface running RIP.
   Status
      Status of RIP on the VLAN interface.
   Send mode
      Format of the RIP updates: RIP 1, RIP 2, or RIP 2 version 1 compatible.
   Recv mode
      The switch can process RIP 1, RIP 2, or RIP 2 version 1 compatible update messages.
   Metric
      Path "cost," a measurement used to determine the "best" RIP route path: 1 is the best, 15 is the worst, 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
      Number of route entries which were not processed for any reason.
   Last update timeticks
      Number of seconds that have passed since we received an update from this neighbor.
**Viewing RIP interface information**

To display RIP interface information, enter the `show ip rip interface` command at any context level.

**Syntax:**

```
show ip rip interface [ ip-addr | vlan vlan-id ]
```

The resulting display will appear similar to the following:

```
HP Switch(config)# show ip rip interface

RIP interface information

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Status</th>
<th>Send mode</th>
<th>Recv mode</th>
<th>Metric</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>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.2.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>1</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.3.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>1</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100.4.0.1</td>
<td>enabled</td>
<td>V2-only</td>
<td>V2-only</td>
<td>1</td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

You can also display the information for a single RIP VLAN interface, by specifying the VLAN ID for the interface, or by specifying the IP address for the interface.

**Example**

**Example 71 RIP interface output by VLAN**

To show the RIP interface information for VLAN 1000, use the `show ip rip interface vlan vid command`.

```
HP Switch# show ip rip interface vlan 4

RIP configuration and statistics for VLAN 4

RIP interface information for 100.4.0.1

| IP Address : 100.4.0.1 |
| 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 |
```

For definitions of the fields in **Example 71** (page 143), see “Viewing general RIP information” (page 141).

The RIP interface information also includes the following fields:

**Bad packets received**

Number of packets that were received on this interface and were not processed for any reason.
Bad routes received
Number of route entries that were received on this interface and were not processed for any reason.

Sent updates
Number of RIP routing updates that have been sent on this interface.

Example

Example 72 Example of show IP rip interface output by IP address

To show the RIP interface information for the interface with IP address 100.2.0.1, enter the show ip rip interface command:

```
HP Switch# show ip rip interface 100.2.0.1
```

RIP interface information for 100.2.0.1

```
IP Address : 100.2.0.1
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
```

Viewing RIP peer information

To display RIP peer information, enter the show ip rip peer command at any context level. The resulting display will appear similar to the following:

Example 73 Example of show IP rip peer output

```
HP Switch# show ip rip peer
RIP peer information
IP Address    Bad routes Last update timeticks
-------------- ----------- ---------------------
100.1.0.100    0           1
100.2.0.100    0           0
100.3.0.100    0           2
100.10.0.100   0           1
```

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.

To show the RIP peer information for a specific peer with IP address 100.1.0.100, enter `show ip rip peer 100.1.0.100`. 
Example 74 Example of show IP rip peer  ip-addr  output

<table>
<thead>
<tr>
<th>HP Switch# show ip rip peer 100.0.1.100</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP peer information for 100.0.1.100</td>
</tr>
<tr>
<td>IP Address : 100.1.0.100</td>
</tr>
<tr>
<td>Bad routes : 0</td>
</tr>
<tr>
<td>Last update timeticks : 2</td>
</tr>
</tbody>
</table>

This display lists information in the fields described above (IP address, Bad routes, Last update timeticks).

Viewing RIP redistribution information

To display RIP redistribution information, enter the `show ip rip redistribute` command at any context level:

Example 75 Example of show IP rip redistribute output

<table>
<thead>
<tr>
<th>HP Switch# show ip rip redistribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP redistributing</td>
</tr>
<tr>
<td>Route type Status</td>
</tr>
<tr>
<td>--------  ------</td>
</tr>
<tr>
<td>connected enabled</td>
</tr>
<tr>
<td>static disabled</td>
</tr>
<tr>
<td>ospf      disabled</td>
</tr>
</tbody>
</table>

RIP automatically redistributes connected routes that are configured on interfaces that are running RIP and all routes that are learned via RIP. The `router rip redistribute` command (page 139), configures the routing switch to cause RIP to advertise connected routes that are not running RIP, static routes, and OSPF routes. The display shows whether RIP redistribution is enabled or disabled for connected, static, and OSPF routes.

Viewing RIP redistribution filter (restrict) information

To display RIP restrict filter information, enter the `show ip rip restrict` command at any context level:

Example 76 Example of show IP rip restrict output

<table>
<thead>
<tr>
<th>HP Switch# show ip rip restrict</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP restrict list</td>
</tr>
<tr>
<td>IP Address          Mask</td>
</tr>
<tr>
<td>------------------- -----------</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

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 (see “Configuring for redistribution” (page 139)).

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 an 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.

The switches support the following RIP types:

- Version 1
- V1 compatible with V2
- Version 2 (the default)

**NOTE:** 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 16 (page 146) lists the global RIP parameters and their default values.

**Table 16 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, connected, and OSPF routes. (RIP redistributes connected routes by default, when RIP is enabled.)</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

#### RIP interface parameters

Table 17 (page 147) lists the VLAN interface RIP parameters and their default values.
### Table 17 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 or 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 address     | The routes that a routing switch learns or advertises can be controlled.     | The routing switch learns and advertises all RIP routes on all RIP interfaces |
| loop prevention| 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:  
• **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 "infinite" or "unreachable") to a route before advertising it on the same interface as the one on which the routing switch learned the route. | Poison reverse |
| receive        | Define the RIP version for incoming packets                                  | V2-only  |
| send           | Define the RIP version for outgoing packets                                  | V2-only  |

## Configuring RIP redistribution

You can configure the routing switch to redistribute connected, static, and OSPF 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.

## Defining RIP redistribution filters

Route redistribution imports and translates different protocol routes into a specified protocol type. On the switches, redistribution is supported for static routes, directly connected routes, and OSPF routes. Redistribution of any other routing protocol into RIP is not currently supported. When you configure redistribution for RIP, you can specify that static, connected, or OSPF routes are imported into RIP routes. Likewise, OSPF redistribution supports the import of static, connected, or RIP routes into OSPF routes.
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.
### Table 18 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] ip routing</td>
<td>Executed at the global configuration level to enable IP routing on the routing switch.</td>
<td>Disabled</td>
<td>(page 152)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router ospf [ enable</td>
<td>disable ]</td>
<td>Executed at the global configuration level to enable OSPF on the routing switch and to enter the OSPF router context.</td>
<td>Disabled</td>
<td>(page 153)</td>
</tr>
<tr>
<td>[no] rfc1583-compatibility</td>
<td>Executed at the global configuration level to toggle routing switch operation compliance between RFC 1583 and RFC 2328.</td>
<td>Compliance enabled</td>
<td>(page 153)</td>
<td>-</td>
</tr>
<tr>
<td>area [ ospf-area-id ] [ backbone</td>
<td>normal]</td>
<td>[no area [ ospf-area-id</td>
<td>backbone ]</td>
<td>Execute to assign the routing switch to a backbone or other normal area.</td>
</tr>
<tr>
<td>area ospf-area-id stub 0-16777215 [no-summary] area ospf-area-id nssa 0-16777215 [no-summary]</td>
<td>[metric-type[ type1</td>
<td>type2 ]] No area ospf-area-id</td>
<td>Execute to assign the routing switch to a stub area or NSSA.</td>
<td>No areas</td>
</tr>
<tr>
<td>vlan vid # ip ospf [ ip-addr</td>
<td>all</td>
<td>area ospf-area-id</td>
<td>Executed in a specific VLAN context to assign the VLAN or individual subnets in the VLAN to the specified area.</td>
<td>-</td>
</tr>
<tr>
<td>interface loopback 0-7 ip ospf lo-ipaddress area ospf-area-id</td>
<td>Executed in a specific loopback context to assign a loopback interface to the specified OSPF area.</td>
<td>-</td>
<td>(page 158)</td>
<td>-</td>
</tr>
<tr>
<td>interface loopback 0-7 # ip ospf lo-ipaddress cost ospf-area-id</td>
<td>Executed in a specific loopback context to modify the cost used to advertise the loopback address (and subnet) to the area border router (ABR).</td>
<td>-</td>
<td>(page 158)</td>
<td>-</td>
</tr>
<tr>
<td>router ospf restrict ip-addr/mask-length</td>
<td>Prevents distribution of the specified range of external routes through an ASBR from sources external to the OSPF domain.</td>
<td>Allow all supported, external route sources</td>
<td>(page 160)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router ospf redistribute [ connected</td>
<td>static</td>
<td>rip ] route-map name</td>
<td>Executed on an ASBR to globally enable redistribution of the specified route type to the OSPF domain through the area in which the ASBR resides.</td>
<td>-</td>
</tr>
<tr>
<td>router ospf default-metric 0-16777215</td>
<td>Globally assigns the cost metric to apply to all external routes redistributed by the ASBR.</td>
<td>10</td>
<td>(page 161)</td>
<td>-</td>
</tr>
<tr>
<td>router ospf metric-type [ type1</td>
<td>type2 ]</td>
<td>Globally reconfigures the redistribution metric type on an ASBR.</td>
<td>type2</td>
<td>(page 162)</td>
</tr>
<tr>
<td>Command syntax</td>
<td>Description</td>
<td>Default</td>
<td>CLI reference</td>
<td>Menu reference</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>---------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>area ospf-area-id range ip-addr/mask-length [no-advertise][type summary][cost 1-16777215]</td>
<td>Use on a routing switch intended to operate as an ABR for the specified area.</td>
<td>-</td>
<td>(page 162)</td>
<td>-</td>
</tr>
<tr>
<td>distance external</td>
<td>Used in the OSPF configuration context to globally reconfigure the administrative distance priority for the specified route type.</td>
<td>110</td>
<td>(page 165)</td>
<td>-</td>
</tr>
<tr>
<td>[no] trap [ trap-name</td>
<td>Used in the OSPF configuration context to enable or disable OSPF traps.</td>
<td>Disabled</td>
<td>(page 165)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf [ ip-address</td>
<td>Used in the VLAN context to indicate the overhead required to send a packet across an interface.</td>
<td>1</td>
<td>(page 167)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf [ ip-address</td>
<td>Used in the VLAN context to indicate the number of seconds that a neighbor router waits for a hello packet from the specified interface before declaring the interface &quot;down.&quot;</td>
<td>40 seconds</td>
<td>(page 167)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf [ ip-address</td>
<td>Used in the VLAN context to indicate the length of time between the transmission of hello packets from the routing switch to adjacent neighbors.</td>
<td>10 seconds</td>
<td>(page 167)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf [ ip-address</td>
<td>Used in the VLAN context to enable changing the priority of an OSPF router.</td>
<td>1</td>
<td>(page 168)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf [ ip-address</td>
<td>Used in the VLAN context to enable changing the retransmission interval for LSAs on an interface.</td>
<td>5 seconds</td>
<td>(page 168)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf [ ip-address</td>
<td>Used in the VLAN context to enable changing the time it takes to transmit link-state update packets on this interface.</td>
<td>1</td>
<td>(page 168)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf [ip-address] authentication-key octet-string</td>
<td>Used in the VLAN interface context to configure password authentication for all interfaces in the VLAN or for a specific subnet.</td>
<td>Disabled</td>
<td>(page 169)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf md5-auth-key-chain chainname-string</td>
<td>Used in the VLAN interface context to configure MD5 authentication for all interfaces in the VLAN or for a specific subnet.</td>
<td>Disabled</td>
<td>(page 170)</td>
<td>-</td>
</tr>
<tr>
<td>ip ospf area area-id virtual-link ip-address</td>
<td>Used on a pair of ABRs at opposite ends of a virtual link in the same area to configure the virtual link connection.</td>
<td>-</td>
<td>(page 171)</td>
<td>-</td>
</tr>
<tr>
<td>area area-id virtual link ip-address dead-interval 1-65535</td>
<td>Used in the router OSPF context on both ABRs in a virtual link to change the number of seconds that a neighbor router waits for a hello packet from the specified interface</td>
<td>40 seconds</td>
<td>(page 172)</td>
<td>-</td>
</tr>
<tr>
<td>Command syntax</td>
<td>Description</td>
<td>Default</td>
<td>CLI reference</td>
<td>Menu reference</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>----------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td><code>area area-id virtual link ip-address hello-interval 1-65535</code></td>
<td>Indicates the length of time between the transmission of hello packets between the ABRs on opposite ends of the virtual link.</td>
<td>10 seconds</td>
<td>(page 172)</td>
<td>-</td>
</tr>
<tr>
<td><code>area area-id virtual link ip-address retransmit-interval 1-3600</code></td>
<td>Used in the router OSPF context on both ABRs in a virtual link to change the number of seconds between LSA retransmissions on the virtual link.</td>
<td>5 seconds</td>
<td>(page 173)</td>
<td>-</td>
</tr>
<tr>
<td><code>area area-id virtual link ip-address transit-delay 0-3600</code></td>
<td>Used in the router OSPF context on both ABRs in a virtual link to change the estimated number of seconds it takes to transmit a link state update packet over a virtual link.</td>
<td>1 second</td>
<td>(page 173)</td>
<td>-</td>
</tr>
<tr>
<td><code>area area-id virtual link ip-addr authentication-key octet-string</code></td>
<td>Used to configure password authentication in the router OSPF context on both ABRs in a virtual link.</td>
<td>Disabled</td>
<td>(page 174)</td>
<td>-</td>
</tr>
<tr>
<td><code>[no] ip ospf md5-auth-key-chain chainname-string</code></td>
<td>Used to configure MD5 authentication in the router OSPF context on both ABRs in a virtual link.</td>
<td>Disabled</td>
<td>(page 175)</td>
<td>-</td>
</tr>
<tr>
<td><code>[no] ip ospf ip-addr passive</code></td>
<td>Configures passive OSPF for an AS.</td>
<td>Active</td>
<td>(page 175)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip ospf general</code></td>
<td>Displays general information about OSPF.</td>
<td>-</td>
<td>(page 177)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip ospf area [ospf-area-id]</code></td>
<td>Shows information for the specified area.</td>
<td>-</td>
<td>(page 179)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip ospf external-link-state</code></td>
<td>Displays external-link state information.</td>
<td>-</td>
<td>(page 180)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip ospf external-link-state [status] [subset-options]</code></td>
<td>Displays external-link state subset options.</td>
<td>-</td>
<td>(page 180)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip ospf external-link-state [status] advertise</code></td>
<td>Displays the hexadecimal data in the specified LSA packet, the actual contents of the LSAs.</td>
<td>-</td>
<td>(page 180)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip ospf interface [vlan vlan-id] ip-addr ]</code></td>
<td>Displays OSPF interface information.</td>
<td>-</td>
<td>(page 181)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip ospf interface [vlan vlan-id] ip-addr ]</code></td>
<td>Displays interface information for a specific VLAN or IP address.</td>
<td>-</td>
<td>(page 182)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip ospf statistics [vlan vlan-id] ip-address ]</code></td>
<td>Displays the statistics on OSPF packets sent and received on the interfaces in VLANs and/or subnets on an OSPF-enabled routing switch.</td>
<td>-</td>
<td>(page 183)</td>
<td>-</td>
</tr>
<tr>
<td><code>clear ip ospf statistics</code></td>
<td>Clears the OSPF statistics for all VLAN interfaces on the switch and</td>
<td>-</td>
<td>(page 185)</td>
<td>-</td>
</tr>
</tbody>
</table>
### Table 18 Summary of commands (continued)

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ospf link-state [status [subset-options] [advertise[subset-options]]]</td>
<td>Displays the OSPF link-state status information.</td>
<td>-</td>
<td>(page 185)</td>
<td>-</td>
</tr>
<tr>
<td>show ip ospf neighbor</td>
<td>Retrieves detailed information for the specific neighbor only.</td>
<td>-</td>
<td>(page 190)</td>
<td>-</td>
</tr>
<tr>
<td>show ip ospf redistribute</td>
<td>Displays the status of the OSPF redistribution.</td>
<td>-</td>
<td>(page 191)</td>
<td>-</td>
</tr>
<tr>
<td>show ip ospf restrict</td>
<td>Displays the status of the OSPF redistribution filters.</td>
<td>-</td>
<td>(page 192)</td>
<td>-</td>
</tr>
<tr>
<td>show ip ospf virtual-link [ area area-id</td>
<td>ip-address ]</td>
<td>Displays OSPF virtual link information.</td>
<td>-</td>
<td>(page 193)</td>
</tr>
<tr>
<td>show ip ospf spf-log</td>
<td>Displays the log used to record SPF calculations on an OSPF-enabled routing switch.</td>
<td>-</td>
<td>(page 194)</td>
<td>-</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>Displays OSPF route information.</td>
<td>-</td>
<td>(page 195)</td>
<td>-</td>
</tr>
<tr>
<td>show ip ospf traps</td>
<td>Lists the OSPF traps currently enabled on the routing switch.</td>
<td>-</td>
<td>(page 197)</td>
<td>-</td>
</tr>
<tr>
<td>debug ip ospf</td>
<td>Turns on the tracing of OSPF packets.</td>
<td>-</td>
<td>(page 197)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip load-sharing 2-4</td>
<td>Enables load-sharing among up to four next-hop routes.</td>
<td>Enabled</td>
<td>(page 197)</td>
<td>-</td>
</tr>
</tbody>
</table>

OSPFv2 is the IPv4 implementation of the Open Shortest Path First protocol. (OSPFv3 is the IPv6 implementation of this protocol.) Beginning with software version K.15.01, the switches can be configured to run OSPFv2 either alone or simultaneously with OSPFv3. (OSPFv2 and OSPFv3 run as independent protocols on the switch and do not have any interaction when run simultaneously.) For overview information on OSPF, see “Overview of OSPF” (page 198).

### Configuring OSPF on the routing switch

#### Enabling IP routing

**Syntax:**

```
[no] ip routing
```

Executed at the global configuration level to enable IP routing on the routing switch.

Default: Disabled

The `no` form of the command disables IP routing. (Global OSPF and RIP routing must be disabled before you disable IP routing.)

**Example**

HP Switch(config)# ip routing
Enabling global OSPF routing

Syntax:

```
[no] router ospf [ enable | disable ]
```

Executed at the global configuration level to enable OSPF on the routing switch and to enter the OSPF router context. This enables you to proceed with assigning OSPF areas, including area border router (ABR) and autonomous system boundary router (ASBR) configuration, and to modify OSPF global parameter settings as needed.

The `enable` form of the command enables OSPF routing, and the `disable` form of the command disables OSPF routing.

Global IP routing must be enabled before executing this command.

Default: Disabled

The `no` form of the command deletes all protocol specific information from the global context and interface context. All protocol parameters are set to default values.

**NOTE:** If you disable OSPF, the switch retains all the configuration information for the disabled protocol in flash memory. If you subsequently restart OSPF, the existing configuration will be applied. After restarting OSPF, the exiting configuration will be applied and the protocol will be in the disabled state.

**Example**

**Example 77 To enter the OSPF router context**

```
HP Switch(config)#router ospf
HP Switch(ospf)#
```

**Example 78 To enable OSPF routing**

```
HP Switch(config)#router ospf enable
HP Switch(ospf)#
```

**Example 79 To disable OSPF routing**

```
HP Switch(config)#router ospf disable
HP Switch(ospf)#
```

**NOTE:** The `no router ospf enable` command also disables OSPF routing.

To delete all protocol-specific information from the global context and interface context and set all protocol parameters to default values:

```
HP Switch(config)#no router ospf
HP Switch(ospf)#
```

**Changing the RFC 1583 OSPF compliance setting**

For more information on this setting, see “Changing the RFC 1583 OSPF compliance setting” (page 209).

**Syntax:**

```
[no] rfc1583-compatibility
```

Executed at the global configuration level to toggle routing switch operation compliance between RFC 1583 and RFC 2328.
rfc1583-compatibility
Configures the routing switch for external route preference rules compliant with RFC 1583.

no rfc1583-compatibility
Configures the routing switch for external route preference rules compliant with RFC 2328.
Default: Compliance enabled

Example
To disable RFC 1583 compatibility on a routing switch in an OSPF domain where RFC 2178 and RFC 2328 are universally supported:

```
HP Switch(config)# router ospf
HP Switch(ospf)# no rfc1583-compatibility
```

Figure 24 Changing external route preference compatibility from RFC 1583 to RFC 2328

```
HP Switch(config)# router ospf
HP Switch(ospf)# no rfc1583-compatibility
HP Switch_8212(ospf)# show ip ospf general
OSPF General Status
  OSPF protocol : enabled
  Router ID : 10.10.51.1
  RFC 1583 compatibility : non-compatible
  Intra-area distance : 110
  Inter-area distance : 110
  AS-external distance : 110
  Default import metric : 10
  Default import metric type : external type 2
  Area Border : no
  AS Border : yes
  External LSA Count : 9
  External LSA Checksum Sum : 408218
  Originate New LSA Count : 24814
  Receive New LSA Count : 14889
```

Assigning the routing switch to OSPF areas
For more information, see “Assigning the routing switch to OSPF areas” (page 209).

Configuring an OSPF backbone or normal area

**Syntax:**
```
area [(ospf-area-id) | [backbone]] [normal] [[ospf-area-id] | [backbone]]
```

After using `router ospf` to globally enable OSPF and enter the global OSPF context, execute this command to assign the routing switch to a backbone or other normal area.

The `no` form of the command removes the routing switch from the specified area.
Default: No areas; Range: 1 to16 areas (of all types)

**ospf-area-id**
Specifies a normal area to which you are assigning the routing switch. You can assign the routing switch to one or more areas, depending on the area in which you want each configured VLAN or subnet to reside.
You can enter area IDs in either whole number or dotted decimal format. (The routing switch automatically converts whole numbers to the dotted decimal format.)

For example, if you enter an area-ID of 1, it appears in the switch's configuration as 0.0.0.1 and an area-ID of 256 appears in the switch configuration as 0.0.1.0.

An area ID can be a value selected to match the IP address of a VLAN belonging to the area or a value corresponding to a numbering system you devise for the areas in a given autonomous system (AS).

Entering an area ID of 0 or 0.0.0.0 automatically joins the routing switch to the backbone area.

The maximum area ID value is 255.255.255.254 (4,294,967,294).

**backbone**

Assigns the routing switch to the backbone area and automatically assigns an area ID of 0.0.0.0 and an area type of normal.

Using 0 or 0.0.0.0 with the above ospf-area-id option achieves the same result. The backbone area is automatically configured as a "normal" area type.

**Example**

To configure a backbone and a normal area with an ID of "1" (0.0.0.1) on a routing switch:

```
HP Switch(ospf)# area backbone
HP Switch(ospf)# area 1
```

**Configuring a stub or NSSA area**

**Syntax:**

```
area ospf-area-id stub 0-16777215 [no-summary]
area ospf-area-id nssa 0-16777215 [no-summary] [metric-type [type1 | type2]]
No area ospf-area-id
```

After using router ospf to globally enable OSPF and enter the global OSPF context, execute this command to assign the routing switch to a stub area or NSSA. (Does not apply to backbone and normal OSPF area ABRs.)

The no form of the command removes the routing switch from the specified area.

**Default:** No areas; Range: 1 to 16 areas (of all types)

**ospf-area-id**

Same area ID as in “Configuring an OSPF backbone or normal area” (page 154), except you cannot assign a backbone area number (0 or 0.0.0.0) to a stub or NSSA area.

```
[ stub | nssa ]
```

Designates the area identified by ospf-area-id as a stub area or NSSA.

```
0-16777215
```

If the routing switch is used as an ABR for the designated area, assigns the cost of the default route (to the backbone) that is injected into the area.

**NOTE:** If the routing switch is not an ABR for the stub area or NSSA, the above cost setting is still required by the CLI, but is not used.
In the default configuration, a routing switch acting as an ABR for a stub area or NSSA injects type-3 summary routes into the area. For an NSSA, the routing switch also injects a type-7 default route into the area.

[no-summary]

Where the routing switch is an ABR for a stub area or an NSSA, this option reduces the amount of link-state advertisement (LSA) traffic entering the area from the backbone by replacing the injection of type-3 summary routes with injection of a type-3 default summary route.

For NSSAs, this command also disables injection of the type-7 default external route from the backbone into the area (included in the metric-type operation described below).

Default: Disabled

For more on this topic, see “Not-so-stubby-area (NSSA)” (page 203), “Stub area” (page 203), and “Replacing type-3 summary LSAs and type-7 default external LSAs with a type-3 default route LSA” (page 205).

[metric-type{ type1 | type2 }]

Used in NSSA ABRs only.

Enables injection of the type-7 default external route and type-3 summary routes into the area instead of a type 3 default route. Also specifies the type of internal cost metric to include in type-7 LSAs advertised for redistribution of external routes in the NSSA. (The redistribution—or external—cost metric is a global setting on the routing switch set by the default-metric command.)

The metric-type command specifies whether to include the redistribution cost in the cost metric calculation for a type-7 default LSA injected into the area.

type1

Calculate external route cost for a type-7 default LSA as the sum of (1) the external route cost assigned by the ASBR plus (2) the internal cost from the router with traffic for the external route to the ASBR advertising the route.

type2

Calculate external route cost for a type-7 default LSA as being only the cost from the router with traffic for the external route to the ASBR advertising the route.

If metric-type is not specified, the default (type2) will be used.

Using the area ospf-area-id nssa 0-16777215 without entering either no-summary or metric-type resets the routing switch to the state where injection of type-3 summary routes and the type-7 default external routes is enabled with metric-type set to type2.

Default: Enabled with metric-type type2

NOTE: Different routers in the NSSA can be configured with different metric-type values.

Examples

The following examples of configuring a stub area and an NSSA on a routing switch use an (arbitrary) cost of "10".
Assigning VLANs and/or subnets to each area

After you define an OSPF area (page A-25), you can assign one or more VLANs and/or subnets to it. When a VLAN is assigned to an area, all currently configured IP addresses in that VLAN are automatically included in the assignment unless you enter a specific IP address.

**NOTE:** All static VLANs configured on a routing switch configured for OSPF must be assigned to one of the defined areas in the AS.

**Syntax:**

```
vlan vid # ip ospf [ ip-addr | all ] area ospf-area-id
```

Executed in a specific VLAN context to assign the VLAN or individual subnets in the VLAN to the specified area. Requires that the area is already configured on the routing switch (page A-25).

When executed without specifying an IP address or using the all keyword, this command assigns all configured networks in the VLAN to the specified OSPF area.

- **vlan vid**
  - Defines the VLAN context for executing the area assignment.

- **ip-addr**
  - Defines a specific subnet on the VLAN to assign to a configured OSPF area.

- **all**
  - Assigns all subnets configured on the VLAN to a configured OSPF area.

- **area ospf-area-id**
  - Identifies the OSPF area to which the VLAN or selected subnet should be assigned.
NOTE: If you add a new subnet IP address to a VLAN after assigning the VLAN to an OSPF area, you must also assign the new subnet to an area:

- If all subnets in the VLAN should be assigned to the same area, just execute `ip ospf area ospf-area-id`.
- But if different subnets belong in different areas, you must explicitly assign the new subnet to the desired area.

Also, to assign a VLAN to an OSPF area, the VLAN must be configured with at least one IP address. Otherwise, executing this command results in the following CLI message:

OSPF can not be configured on this VLAN.

Example

To assign VLAN 8 on a routing switch to area 3 and include all IP addresses configured in the VLAN, enter the following commands:

```
HP Switch(ospf)# vlan 8
HP Switch(vlan-8)# ip ospf area 3
```

Suppose that a system operator wants to assign the three subnets configured in VLAN 10 as shown below:

- 10.10.10.1 to OSPF area 5
- 10.10.11.1 to OSPF area 5
- 10.10.12.1 to OSPF area 6

The operator could use the following commands to configure the above assignments:

```
HP Switch(ospf)# vlan 10
HP Switch(vlan-10)# ip ospf 10.10.10.1 area 5
HP Switch(vlan-10)# ip ospf 10.10.11.1 area 5
HP Switch(vlan-10)# ip ospf 10.10.12.1 area 6
```

Assigning loopback addresses to an area (optional)

After you define the OSPF areas to which the switch belongs, you can assign a user-defined loopback address to an OSPF area. A loopback interface is a virtual interface configured with an IP address and is always reachable as long as at least one of the IP interfaces on the switch is operational. Because the loopback interface is always up, you ensure that the switch's router ID remains constant and that an OSPF network is protected from changes caused by downed interfaces.

For more information about how to configure a loopback interface, see "Configuring a Loopback Interface" in chapter "Configuring IP Addressing," in the Management and Configuration Guide for your routing switch.

Syntax:

```
interface loopback 0-7 ip ospf lo-ipaddress area ospf-area-id
```

Executed in a specific loopback context to assign a loopback interface to the specified OSPF area. Requires that the specified loopback interface is already configured with an IP address on the switch.

```
interface loopback 0-7
  ip ospf lo-ipaddress
```

 Defines the loopback context for executing the area assignment.
area ospf-area-id

Identifies the OSPF area to which the loopback interface is assigned.
You can enter a value for the OSPF area in the format of an IP address or a number in the range 0 to 4,294,967,295.

Example

To assign user-defined loopback interface 3 on the switch to area 192.5.0.0 and include the loopback IP address 172.16.112.2 in the OSPF broadcast area, enter the following commands:

HP Switch(config)# interface loopback 3
HP Switch(lo-3)# ip ospf 172.16.112.2 area 192.5.0.0

Syntax:

interface loopback 0-7# ip ospf lo-ip-address cost number

Executed in a specific loopback context to modify the cost used to advertise the loopback address (and subnet) to the area border router (ABR). Requires that the specified loopback interface is already configured with an IP address on the switch.

loopback interface 0-7

Defines the loopback context for executing the cost assignment.

ip ospf lo-ip-address

Specifies the loopback interface by its IP address.

cost number

Specifies a number that represents the administrative metric associated with the loopback interface. Valid values are from 1 to 65535.
Default: 1.

Example

To configure a cost of 10 for advertising the IP address 172.16.112.2 configured for loopback interface 3 in an OSPF area 192.5.0.0, enter the following commands:

HP Switch(config)# interface loopback 3
HP Switch(lo-3)# ip ospf 172.16.112.2 area 192.5.0.0
HP Switch(lo-3)# ip ospf 172.16.112.2 cost 10

OSPF redistribution of loopback addresses

When you assign a loopback address to an OSPF area, the route redistribution of the loopback address is limited to the specified area.

When route redistribution is enabled:

- The switch advertises a loopback IP address that is not assigned to an OSPF area as an OSPF external route to its OSPF neighbors, and handles it as a connected route.

- The switch advertises a loopback address that is assigned to an OSPF area as an OSPF internal route.

To enable redistribution of loopback IP addresses in OSPF, enter the redistribution connected command as described in “Enabling route redistribution” (page 161).
Example 80 Assigning loopback IP addresses to OSPF areas

The loopback IP address 13.3.4.5 of loopback 2 is advertised only in OSPF area 0.0.0.111. The IP addresses 14.2.3.4 and 15.2.3.4 of loopback 1 are advertised in all OSPF areas. The lines in bold below show that the IP address of loopback interface 2 is assigned to OSPF area 111.

HP Switch(config)# interface loopback 1
HP Switch(lo-1)# ip address 14.2.3.4
HP Switch(lo-1)# ip address 15.2.3.4
HP Switch(lo-1)# exit
HP Switch(config)# interface loopback 2
HP Switch(lo-2)# ip address 13.3.4.5
HP Switch(lo-2)# ip ospf 15.2.3.4 area 0.0.0.111
HP Switch(lo-2)# exit

Example 81 Verifying OSPF redistribution of loopback interfaces

To verify the OSPF redistribution of loopback interfaces, enter the `show ip route` command from any context level to display IP route table entries.

In this example, a loopback address assigned to an area is displayed as an `ospf intra-area (internal)` route to its neighbor; a loopback address not assigned to a specific area is displayed as an `ospf external` route:

HP Switch(config)# show ip route

```
IP Route Entries
Destination     Gateway      VLAN  Type  Sub-Type   Metric   Dist
-----------     -------      ----  ----  --------   ------   ----
20.0.15.1/32   25.0.67.131   25    ospf  external2   10      110
20.0.16.2/32   25.0.67.131   25    ospf  intra-area  10      110
```

Configuring external route redistribution in an OSPF domain (optional)

For more information, see “Configuring for external route redistribution in an OSPF domain” (page 210).

Configuring redistribution filters

**Syntax:**

```
router ospf restrict ip-addr/mask-length
```

Prevents distribution of the specified range of external routes through an ASBR from sources external to the OSPF domain.

Default: Allow all supported, external route sources

**NOTE:** Use this command to block unwanted, external routes before enabling route redistribution on the ASBR.

**Example**

To configure a routing switch operating as an ASBR to filter out redistribution of static, connected, or RIP routes on network 10.0.0.0, enter the following commands:

```
HP Switch(config)# router ospf restrict 10.0.0.0/8
```

**NOTE:** In the default configuration, redistribution is permitted for all routes from supported sources.
Enabling route redistribution

This step enables ASBR operation on a routing switch, and must be executed on each routing switch connected to external routes you want to redistribute in your OSPF domain.

The basic form of the redistribute command redistributes all routes of the selected type. For finer control over route selection and modification of route properties, you can specify the route-map parameter and the name of a route map. (For general information on route policy and route maps, see “Route Policy” (page 215). For examples of using route maps in route redistribution, see “Using route policy in route redistribution” (page 225).)

**NOTE:** Do not enable redistribution until you have configured the redistribution "restrict" filters. Otherwise, the network might become overloaded with routes that you did not intend to redistribute.

**Syntax:**

\[
\text{[no] router ospf redistribute [ connected | static | rip ] route-map name}
\]

Executed on an ASBR to globally enable redistribution of the specified route type to the OSPF domain through the area in which the ASBR resides.

- **static**
  - Redistribute from manually configured routes.

- **connected**
  - Redistribute from locally connected networks.

- **rip**
  - Redistribute from RIP routes.

- **route-map name**
  - Optionally specify the name of a route-map to apply during redistribution.

The no form of the command disables redistribution for the specified route type.

**Example**

To enable redistribution of all supported external route types through a given ASBR, execute the following commands.

```
HP Switch(config)# router ospf redistribution connected
HP Switch(config)# router ospf redistribution static
HP Switch(config)# router ospf redistribution rip
```

Modifying the default metric for redistribution (optional)

The default metric is a global parameter that specifies the cost applied to all OSPF routes by default.

**Syntax:**

```
router ospf default-metric 0-16777215
```

Globally assigns the cost metric to apply to all external routes redistributed by the ASBR. By using different cost metrics for different ASBRs, you can prioritize the ASBRs in your AS.

Default: 10

**Example**

To assign a default metric of 4 to all routes imported into OSPF on an ASBR, enter the following commands:
Modifying the redistribution metric type (optional)

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.

**Syntax:**

```
router ospf metric-type [ type1 | type2 ]
```

Globally reconfigures the redistribution metric type on an ASBR.

- **type1**
  - Specifies the OSPF metric plus the external metric for an external route.

- **type2**
  - Specifies the external metric for an external route.

Default: type2

**Example**

To change from the default setting on an ASBR to type 1, enter the following command:

```
HP Switch(config)# router ospf metric-type type1
```

Configuring ranges on an ABR to reduce advertising to the backbone (optional)

For more information, see “Configuring ranges on an ABR to reduce advertising to the backbone (optional)” (page 210).

**Syntax:**

```
area [ospf-area-id | [backbone]] range
  [[ip-addr/mask-length]] [no-advertise] [type summary [ [cost 1-16777215] | nssa ] [cost 1-16777215]]
area ospf-area-id range ip-addr/mask-length [no-advertise] [type summary [ [cost 1-16777215] | nssa ]]
```

Use this command on a routing switch intended to operate as an ABR for the specified area to do either of the following:

- Simultaneously create the area and corresponding range setting for routes to summarize or block.
- For an existing area, specify a range setting for routes to summarize or block.

**ospf-area-id**

- Same area ID as in “Configuring an OSPF backbone or normal area” (page 154), except you cannot assign a backbone area number (0 or 0.0.0.0) to a stub or NSSA area.

**range ip-addr/mask-length**

- Defines the range of route advertisements to either summarize for injection into the backbone area or to prevent from being injected into the backbone area.
- The ip-addr value specifies the IP address portion of the range, and mask-length specifies the leftmost significant bits in the address.
The ABR for the specified area compares the IP address of each outbound route advertisement with the address and significant bits in the mask to determine which routes to select for either summarizing or blocking.

For example, a range of 10.10.32.1/14 specifies all routes in the range of 10.10.32.1 - 10.10.35.254.

[no-advertise]
Use this keyword only if you want to configure the ABR to prevent advertisement to the backbone of a specified range of routes. (This has the effect of “hiding” the specified range from the backbone area.)

If you do not use this option, the ABR advertises the specified range of routes according to the type summary | nssa selection described below.

[type summary [ [cost 1-16777215] | nssa ]]
Configures the type of route summaries to advertise or block. If type is not used in the command, the ABR defaults this setting to summary.

type summary [ [cost 1-16777215] ]
Specifies internal routes in the configured range of RAs. If no-advertise (above) is used in the command, the ABR prevents the selected internal routes from being summarized in a type-3 LSA and advertised to the backbone.

If no-advertise is not used in the command, the selected routes are summarized to the backbone in a type-3 LSA.

[cost 1-16777215]
User-configured cost for an area summary range. If cost is specified, the range will advertise the specified cost instead of the calculated cost.

nssa
Specifies external routes (type-7 LSAs) in the configured range of route advertisements. If no-advertise (above) is used in the command, the ABR prevents the selected external routes from being summarized in a type-5 LSA and advertised to the backbone. (Configure this option where an ABR for an NSSA advertises external routes that you do not want propagated to the backbone.)

If no-advertise is not used in the command, the selected routes learned from type-7 LSAs in the area are summarized to the backbone in a type-5 LSA.

[cost 1-16777215]
User configured cost for an NSSA summary range. If cost is not configured, the ABR will use the algorithm defined in RFC 3101 to compute the cost and metric-type of the summarized route. If cost is specified, then the range will advertise the specified cost as the cost of the summarized route.

Assigning a cost
The cost parameter provides a way to define a fixed, user-assigned cost of an LSA type 3 summarized prefix.
Example 82 Setting a summary cost to an area

This example shows how to set the summary cost to 100 for area 10 with an address range of 10.10.0.0/16.

HP Switch(ospf)# area 10 range 10.10.0.0/16 type summary cost 100

Example 83 Using a standard summary cost for an area

This example shows how to use the standard method for determining the summarized cost.

HP Switch(ospf)# area 10 range 10.10.0.0/16 type summary

You must execute write mem to preserve these settings across reboots.

Example 84 Setting a summary cost to an NSSA area

To set the summary cost for NSSA area 20 address range 10.20.0.0/16 to 100 with a default metric-type of type2, enter the following command.

HP Switch(ospf)# area 20 range 10.20.0.0/16 type nssa cost 100

Example 85 Setting a summary cost and metric-type to an NSSA area

To set the summary cost and metric-type for NSSA area 20 address range 10.20.0.0/16 to 100, enter the following command.

HP Switch(ospf)# area 10 range 10.10.0.0/16 type nssa cost 100 metric-type type1

Example 86 Using the RFC standard method to determine the summarized cost to an NSSA area

To change the configuration so that the 10.20.0.0/16 range uses the RFC standard method for determining the summarized cost, enter the following command.

HP Switch(ospf)# area 10 range 10.10.0.0/16 type nssa

You must execute write mem to preserve these settings across reboots.

Example 87 Output showing settings for summary costs

The show ip ospf command displays information about summary costs. An entry of auto indicates that the cost is calculated by the OSPF standard for summarized networks.

HP Switch(config)# show ip ospf

OSPF Configuration Information

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>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.10</td>
<td>Summary</td>
<td>10.10.0.0</td>
<td>255.255.0.0</td>
<td>yes</td>
<td>auto</td>
</tr>
<tr>
<td>0.0.0.20</td>
<td>NSSA</td>
<td>10.20.0.0</td>
<td>255.255.0.0</td>
<td>yes</td>
<td>auto</td>
</tr>
<tr>
<td>0.0.0.30</td>
<td>Summary</td>
<td>10.30.0.0</td>
<td>255.255.0.0</td>
<td>no</td>
<td>16777215</td>
</tr>
</tbody>
</table>

Example 88 Defining a range of internal routes to advertise to the backbone

The commands in this example define the same range of internal routes in area 30 to summarize for injection into the backbone area. (In this example, area 30 can be a normal or stub area, or an NSSA.)

HP Switch(ospf)# area 30 range 10.0.0.0/8
HP Switch(ospf)# area 30 range 10.0.0.0/8 type summary
Example 89 Defining a range of internal routes to block from advertising to the backbone

For the same range of routes, you can use either of the following commands to block injection of a range of summary routes (type-3 LSAs) from area 30 into the backbone.

HP Switch(config)# area 30 range 10.0.0.0/8 type no-advertise
HP Switch(config)# area 30 range 10.0.0.0/8 type no-advertise summary

Allowing or blocking a range of external routes available through an ASBR in an NSSA

Example 90 Example of allowing or blocking a range of external RAs to the backbone

This example applies only to external routes that can be advertised from an NSSA to the backbone. The first command defines the range of external routes in the Area 7 NSSA to advertise to the backbone. The second command defines the range of external routes in the Area 7 NSSA to block from advertising to the backbone.

HP Switch(config)# area 7 range 192.51.0.0/16 type nssa
HP Switch(config)# area 7 range 192.51.0.0/16 no-advertise type nssa

Influencing route choices by changing the administrative distance default (optional)

For more information, see “Influencing route choices by changing the administrative distance default (optional)” (page 210).

Syntax:

\[ \text{distance [ external | inter-area | intra-area 1-255 ]} \]

Used in the OSPF configuration context to globally reconfigure the administrative distance priority for the specified route type.

1 is the highest priority; 255 is the lowest priority.

\[ \text{external 1-255} \]

Changes the administrative distance for routes between the OSPF domain and other EGP domains.

\[ \text{inter-area 1-255} \]

Changes the administrative distance for routes between areas within the same OSPF domain.

\[ \text{intra-area 1-255} \]

Changes the administrative distance for routes within OSPF areas.

Default: 110; range: 1–255

Changing OSPF trap generation choices (optional)

OSPF traps (defined by RFC 1850) are supported on the routing switches. OSPF trap generation is disabled by default, but you can use the following command to enable generation of any or all of the supported OSPF traps.

Syntax:

\[ \text{[no] trap [ trap-name | all ]} \]

Used in the OSPF configuration context to enable or disable OSPF traps.

\[ \text{all} \]

 Enables or disables all OSPF traps available on the routing switch.
trap-name

Specifies a trap from table “OSPF traps and associated MIB objects” (page 166) to enable or disable.

The no form disables the specified trap.

Default: All OSPF traps disabled

Table “OSPF traps and associated MIB objects” (page 166) summarizes OSPF traps supported on the switches, and their associated MIB objects from RFC 1850.

**Table 19 OSPF traps and associated MIB objects**

<table>
<thead>
<tr>
<th>OSPF trap name</th>
<th>MIB object</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-authentication-failure</td>
<td>ospflfAuthFailure</td>
</tr>
<tr>
<td>interface-config-error</td>
<td>ospflfConfigError</td>
</tr>
<tr>
<td>interface-receive-bad-packet</td>
<td>ospflfrxBadPacket</td>
</tr>
<tr>
<td>interface-retransmit-packet</td>
<td>ospfTxRetransmit</td>
</tr>
<tr>
<td>interface-state-change</td>
<td>.</td>
</tr>
<tr>
<td>neighbor-state-change</td>
<td>ospfNbrStateChange</td>
</tr>
<tr>
<td>originate-lsa</td>
<td>ospfOriginateLsa</td>
</tr>
<tr>
<td>originate-maxage-lsa</td>
<td>ospfMaxAgeLsa</td>
</tr>
<tr>
<td>virtual-interface-authentication-failure</td>
<td>.</td>
</tr>
<tr>
<td>virtual-interface-config-error</td>
<td>ospfVirtlfConfigError</td>
</tr>
<tr>
<td>virtual-interface-state-change</td>
<td>ospfVirtlfStateChange</td>
</tr>
<tr>
<td>virtual-neighbor-state-change</td>
<td>ospfVirtNbrStateChange</td>
</tr>
<tr>
<td>virtual-interface-receive-bad-packet</td>
<td>ospfVirtlfRxBadPacket</td>
</tr>
<tr>
<td>virtual-interface-retransmit-packet</td>
<td>ospfVirtlfTxRetransmit</td>
</tr>
</tbody>
</table>

**Example**

**Example 91 Enabling OSPF traps**

If you wanted to monitor the neighbor-state-change and interface-receive-bad-packet traps, you would use the following commands to configure the routing switch to enable the desired trap. The show command verifies the resulting OSPF trap configuration.

```
HP Switch(ospf)# trap neighbor-state-change
HP Switch(ospf)# trap interface-receive-bad-packet
HP Switch(ospf)# show ip ospf traps

OSPF Traps Enabled

==================
Neighbor State Change
Interface Receive Bad Packet
```

Adjusting performance by changing the VLAN or subnet interface settings (optional)

For more information, see “Adjusting performance by changing the VLAN or subnet interface settings (optional)” (page 211)
Indicating the cost per-interface

Syntax:

```
ip ospf [ ip-address | all ] cost 1-65535
```

Used in the VLAN context to indicate 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.

Allows different costs for different subnets in the VLAN.

```
ip ospf cost 1-65535
  Assigns the specified cost to all networks configured on the VLAN.
ip ospf ip-address cost 1-65535
  Assigns the specified cost to the specified subnet on the VLAN.
ip ospf all cost 1-65535
  Assigns the specified cost to all networks configured on the VLAN. (Operates the same as the `ip ospf cost` option, above.)
```

Default: 1; range 1–65535

Indicating the per-interface dead interval

Syntax:

```
ip ospf [ ip-address | all ] dead-interval 1-65535
```

Used in the VLAN context to indicate the number of seconds that a neighbor router waits for a hello packet from the specified interface before declaring the interface "down." Allows different settings for different subnet interfaces in the VLAN.

```
ip ospf dead-interval 1-65535
  Assigns the specified dead interval to all networks configured on the VLAN.
ip ospf ip-address dead-interval 1-65535
  Assigns the specified dead interval to the specified subnet on the VLAN.
ip ospf all dead-interval 1-65535
  Assigns the specified dead interval to all networks configured on the VLAN. (Operates the same as the `ip ospf dead-interval` option, above.)
```

Default: 40 seconds; range 1–65535 seconds

Indicating the per-interface hello interval

Syntax:

```
ip ospf [ ip-address | all ] hello-interval 1-65535
```

Used in the VLAN context to indicate the length of time between the transmission of hello packets from the routing switch to adjacent neighbors.

The value can be from 1 to 65535 seconds. Allows different settings for different subnet interfaces in the VLAN.

```
ip ospf hello-interval 1-65535
  Assigns the specified hello interval to all networks configured on the VLAN.
ip ospf ip-address hello-interval 1-65535
  Assigns the specified hello interval to the specified subnet on the VLAN.
```

Adjusting performance by changing the VLAN or subnet interface settings (optional)
ip ospf all hello-interval 1-65535
  Assigns the specified hello interval to all networks configured on the VLAN.
  Operates the same as the ip ospf hello-interval option.
  Default: 10 seconds; range 1–65535 seconds

Changing priority per-interface

Syntax:

ip ospf [ip-address | all] priority 1-255
The priority is used when selecting the DR and backup DRs (BDRs).
The value can be from 0 to 255 (with 255 as the highest priority). If you set the
priority to 0, the routing switch does not participate in DR and BDR election. Allows
different settings for different subnet interfaces in the VLAN.

ip ospf priority 1-255
  Assigns the specified priority to all networks configured on the VLAN.

ip ospf ip-address priority 1-255
  Assigns the specified priority to the specified subnet on the VLAN.

ip ospf all priority 1-255
  Assigns the specified priority to all networks configured on the VLAN. Operates
  the same as the ip ospf priority option.
  Default: 1; range 0–255

Changing retransmit interval per-interface

Syntax:

ip ospf [ip-address | all] retransmit-interval 0-3600
Used in the VLAN context to enable changing the retransmission interval for LSAs
on an interface. Allows different settings for different subnet interfaces in the VLAN.

ip ospf priority 1-255
  Assigns the specified retransmit interval to all networks configured on the VLAN.

ip ospf ip-address priority 1-255
  Assigns the specified retransmit interval to the specified subnet on the VLAN.

ip ospf all priority 1-255
  Assigns the specified retransmit interval to all networks configured on the VLAN.
  Operates the same as the ip ospf priority option.
  Default: 5 seconds; range: 1–3600 seconds

Changing transit-delay per-interface

Syntax:

ip ospf [ip-address | all] transit-delay 0-3600
Used in the VLAN context to enable changing the time it takes to transmit link-state
update packets on this interface. Allows different settings for different subnet
interfaces in the VLAN.

Default: 1 second; range: 1–3600 seconds

ip ospf transit-delay 1-3600
  Reconfigures the estimated number of seconds it takes to transmit a link-state
  update packet to all networks configured on the VLAN.
ip ospf ip-address transit-delay 1-3600
Reconfigures the estimated number of seconds it takes to transmit a link-state
update packet to all networks configured on the specified subnet on the VLAN.

ip ospf all transit-delay 1-3600
Reconfigures the estimated number of seconds it takes to transmit a link-state
update packet to all networks configured on the VLAN. (Operates the same as
the ip ospf transit-delay option, above.)

Examples of changing per-interface settings

Suppose that VLAN 30 is multinetted, with two subnets in area 1 and one subnet in area 5:

vlan 30
ip ospf 10.10.30.1 area 0.0.0.1
ip ospf 10.10.31.1 area 0.0.0.1
ip ospf 10.10.32.1 area 0.0.0.5

If you wanted to quickly reconfigure per-interface OSPF settings for VLAN 30, such as those listed
below, you could use the commands shown in Figure “Reconfiguring per-interface settings in a
multinetted VLAN” (page 169).

• Assign a cost of "5" to the two subnets in area 1 and a cost of "10" to the subnet in area 5.
• Assign a dead interval of 45 seconds to the subnets in area 1 and retain the default setting
(40 seconds) for the subnet in area 5.

Figure 26 Reconfiguring per-interface settings in a multinetted VLAN

Configuring OSPF interface authentication (optional)
For more information, see “Configuring OSPF interface authentication (optional)” (page 211).

Configuring OSPF password authentication

Syntax:

ip ospf [ip-address] authentication-key key-string
no ip ospf [ip-address] authentication

Used in the VLAN interface context to configure password authentication for all
interfaces in the VLAN or for a specific subnet. The password takes effect
immediately, and all OSPF packets transmitted on the interface contain this
password. All OSPF packets received on the interface are also checked for the
password. If it is not present, the packet is dropped.

To disable password authentication on an interface, use the no form of the
command.

For the 5400zl and 8200zl switches, when the switch is in enhanced secure mode,
commands that take a secret key as a parameter have the echo of the secret typing
replaced with asterisks. The input for key-string is prompted for interactively.

For more information, see the chapter “Secure Mode (5400zl and 8200zl Switches)”
ip-address
   Used in subnetted VLAN contexts where you want to assign or remove a password associated with a specific subnet.
   Omit this option when you want the command to apply to all interfaces configured in the VLAN.

key-string
   An alphanumeric string of one to eight characters. (Spaces are not allowed.)
   To change the password, re-execute the command with the new password.
   Use `show ip ospf interface ip-address` to view the current authentication setting.

**NOTE:** To replace the password method with the MD5 method on a given interface, overwrite the password configuration by using the MD5 form of the command shown in the next syntax description. (It is not necessary to disable the currently configured OSPF password.)

Default: Disabled

### Configuring OSPF MD5 authentication

**Syntax:**

```plaintext
ip ospf md5-auth-key-chain chainname-string
no ip ospf [ip-address] authentication
```

Used in the VLAN interface context to configure MD5 authentication for all interfaces in the VLAN or for a specific subnet. The MD5 authentication takes effect immediately, and all OSPF packets transmitted on the interface contain the designated key. All OSPF packets received on the interface are also checked for the key. If it is not present, the packet is dropped.

To disable MD5 authentication on an interface, use the `no` form of the command.

**NOTE:** Before using this authentication option, you must configure one or more key chains on the routing switch by using the Key Management System (KMS) described in chapter "Key Management System" in the Access Security Guide for your routing switch.

Default: Disabled

ip-address
   Used in subnetted VLAN contexts where you want to assign or remove MD5 authentication associated with a specific subnet.
   Omit this option when you want the command to apply to all interfaces configured in the VLAN.

chain-name-string
   The name of a key generated using the `key-chain chain_name key key_id`.
   To change the MD5 authentication configured on an interface, re-execute the command with the new MD5 key.

Use `show ip ospf interface ip-address` to view the current authentication setting.

**NOTE:** To replace the MD5 method with the password method on a given interface, overwrite the MD5 configuration by using the password form of the command shown in the next syntax description. (It is not necessary to disable the currently configured OSPF MD5 authentication.)
Configuring a virtual link

For information about virtual links, see “Configuring an ABR to use a virtual link to the backbone” (page 211).

Syntax:

```
ip ospf area area-id virtual link ip-address
```

Used on a pair of ABRs at opposite ends of a virtual link in the same area to configure the virtual link connection.

`area-id`

This must be the same for both ABRs in the link and is the area number of the virtual link transit area in either decimal or dotted decimal format.

`ip-address`

On an ABR directly connected to the backbone area, this value must be the IP address of an ABR (in the same area) needing a virtual link to the backbone area as a substitute for a direct physical connection.

On the ABR that needs the virtual link to the backbone area, this value must be the IP address of the ABR (in the same area) having a direct physical connection to the backbone area.

Example

Figure 27 (page 171) shows an OSPF ABR, routing switch "A" that lacks a direct connection to 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, define it on the routers that are at each end of the link. No configuration for the virtual link is required on the other routers on the path through the transit area (such as routing switch "B" in this example).

```
Figure 27 Defining OSPF virtual links within a network
```

To configure the virtual link on routing switch "A," enter the following command specifying the area 1 interface on routing switch "C":

```
HP Switch(ospf)# area 1 virtual-link 209.157.22.1
```
To configure the virtual link on routing switch "C," enter the following command specifying the area 1 interface on routing switch "A":

```
HP Switch(ospf)# area 1 virtual-link 10.0.0.1
```

See “Changing the dead interval on a virtual link” (page 172) for descriptions of virtual link interface parameters you can either use in their default settings or reconfigure as needed.

### Changing the dead interval on a virtual link

For more information, see “Adjusting virtual link performance by changing the interface settings (optional)” (page 212).

**Syntax:**

```
area area-id virtual link ip-address dead-interval 1-65535
```

Used in the router OSPF context on both ABRs in a virtual link to change the number of seconds that a neighbor router waits for a hello packet from the specified interface before declaring the interface "down." This should be some multiple of the hello interval. The dead-interval setting must be the same on both ABRs on a given virtual link.

- **area-id**
  Specifies the OSPF area in which both ABRs in a given virtual link operate. In this use, the area ID is sometimes termed "transit area ID."
  This value must be the same for both ABRs in the virtual link.

- **ip-address**
  For an ABR in a given virtual link, this is the IP address used to create the link on that ABR.
  This IP address matches the IP address of the interface on the opposite end of the virtual link. See the description of *ip-address* in the syntax description under “Configuring a virtual link” (page 171).

Use `show ip ospf virtual-link ip-address` to view the current setting.

Default: 40 seconds; range: 1–65535 seconds

### Indicating the hello interval on a virtual link

**Syntax:**

```
area area-id virtual link ip-address hello-interval 1-65535
```

Used in the router OSPF context on both ABRs in a virtual link to indicate the length of time between the transmission of hello packets between the ABRs on opposite ends of the virtual link.

The hello-interval setting must be the same on both ABRs on a given virtual link.

Default: 10 seconds; range: 1–65535 seconds

- **area-id**
  Specifies the OSPF area in which both ABRs in a given virtual link operate. In this use, the area ID is sometimes termed "transit area ID."
  This value must be the same for both ABRs in the virtual link.

- **ip-address**
  For an ABR in a given virtual link, this is the IP address used to create the link on that ABR. (This IP address matches the IP address of the interface on the opposite end of the virtual link. See the description of *ip-address* in the syntax description under “Configuring a virtual link” (page 171).)
Use `show ip ospf virtual-link ip-address` to view the current setting.

**Changing the retransmitting interval on a virtual link**

*Syntax:*

```
area area-id virtual link ip-address retransmit-interval 1-3600
```

Used in the router OSPF context on both ABRs in a virtual link to change the number of seconds between LSA retransmissions on the virtual link.

The retransmit-interval setting must be the same on both ABRs on a given virtual link. This value is also used when retransmitting database description and link-state request packets.

**area-id**

Specifies the OSPF area in which both ABRs in a given virtual link operate. In this use, the area ID is sometimes termed "transit area ID." This value must be the same for both ABRs in the virtual link.

**ip-address**

For an ABR in a given virtual link, this is the IP address used to create the link on that ABR. (This IP address matches the IP address of the interface on the opposite end of the virtual link. See the description of `ip-address` in the syntax description under “Configuring a virtual link” (page 171).)

Use `show ip ospf virtual-link ip-address` to view the current setting.

Default: 5 seconds; range: 1–3600 seconds

**Changing the transit-delay on a virtual link**

*Syntax:*

```
area area-id virtual link ip-address transit-delay [0-3600]
```

Used in the router OSPF context on both ABRs in a virtual link to change the estimated number of seconds it takes to transmit a link state update packet over a virtual link. The transit-delay setting must be the same on both ABRs on a given virtual link.

**area-id**

Specifies the OSPF area in which both ABRs in a given virtual link operate. In this use, the area ID is sometimes termed "transit area ID." This value must be the same for both ABRs in the virtual link.

**ip-address**

For an ABR in a given virtual link, this is the IP address used to create the link on that ABR. (This IP address matches the IP address of the interface on the opposite end of the virtual link. See the description of `ip-address` in the syntax description under “Configuring a virtual link” (page 171).)

Use `show ip ospf virtual-link ip-address` to view the current setting.

Default: 1 second; range: 1–3600 seconds

**Example**

To change the hello-interval on the virtual link configured for the network in Figure 27 (page 171) to 60 seconds:

- On routing switch "A" (IP address 10.0.0.1) you would use the following command to reconfigure the current hello-interval to 60 seconds:
On routing switch "C" (IP address 209.157.22.1) you would use the following command to reconfigure the current hello-interval to 60 seconds:

```
HP Switch(ospf)# area 1 virtual-link 209.157.22.1 hello-interval 60
```

### Configuring OSPF authentication on a virtual link

For more information, see “Configuring OSPF authentication on a virtual link” (page 212).

### Authenticating the OSPF password on a virtual link

**Syntax:**

```
area area-id virtual-link ip-addr authentication-key key-string no area 1 virtual-link ip-address authentication
```

Used to configure password authentication in the router OSPF context on both ABRs in a virtual link. The password takes effect immediately, and all OSPF packets transmitted on the link contain this password. Every OSPF packet received on the interface for the virtual link on each ABR is checked for the password. If it is not present, the packet is dropped.

To disable password authentication on an ABR interface used for a virtual link, use the no form of the command.

The password must be the same on both ABRs on a given virtual link.

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

- `area-id` Specifies the OSPF area in which both ABRs in a given virtual link operate. In this use, the area ID is sometimes termed "transit area ID." This value must be the same for both ABRs in the virtual link.
- `ip-address` For an ABR in a given virtual link, this is the IP address used to create the link on that ABR. (This IP address matches the IP address of the interface on the opposite end of the virtual link. See the description of `ip-address` in the syntax description under “Configuring a virtual link” (page 171).)
- `key-string` An alphanumeric string of one to eight characters. (Spaces are not allowed.) To change the password, re-execute the command with the new password.

**NOTE:** To replace the password method with the MD5 method on a given interface, overwrite the password configuration by using the MD5 form of the command shown in “Authenticating OSPF MD5 on a virtual link” (page 175). (It is not necessary to disable the currently configured OSPF password.)

Default: Disabled
Authenticating OSPF MD5 on a virtual link

Syntax:

```
ip ospf md5-auth-key-chain chain-name-string no ip ospf [ip-address]
authentication
```

Used to configure MD5 authentication in the router OSPF context on both ABRs in a virtual link. The MD5 authentication takes effect immediately, and all OSPF packets transmitted on the link contain the designated key. Every OSPF packet received on the interface for the virtual link on each ABR is checked for the key. If it is not present, the packet is dropped.

To disable MD5 authentication on an ABR interface used for a virtual link, use the `no` form of the command. The password must be the same on both ABRs on a given virtual link.

**NOTE:** Before using this authentication option, you must configure one or more key chains on the routing switch by using the Key Management System (KMS) described in chapter "Key Management System" in the Access Security Guide for your routing switch.

```
ip-address
```

For an ABR in a given virtual link, this is the IP address used to create the link on that ABR. (This IP address matches the IP address of the interface on the opposite end of the virtual link. See the description of `ip-address` in the syntax description under “Configuring a virtual link” (page 171).)

```
chain-name-string
```

The name of a key generated using the `key-chain` command.

To change the MD5 authentication configured on a virtual link, re-execute the command with the new MD5 key.

**NOTE:** To replace the MD5 method with the password method on a virtual link, overwrite the MD5 configuration by using the password form of the command shown under “Authenticating the OSPF password on a virtual link” (page 174). (It is not necessary to disable the currently configured OSPF MD5 authentication.)

Default: Disabled

Configuring a passive OSPF interface

For more information, see “About OSPF passive” (page 212).

Enter this command in VLAN context:

```
HP Switch(vlan-1)# ip ospf passive
```

**Syntax:**

```
[no] ip ospf ip-addr passive
```

Configures passive OSPF for an AS.

```
ip-addr
```

Optionally, you can configure an IP address on the VLAN.

The `no` option disables the passive option; the interface becomes an active interface.

Default: Active
Example

To display the OSPF passive information, enter the command shown in Figure A-14:

Example 92 show ip ospf interface command with passive configured on an interface

HP Switch(vlan-1)# show ip ospf interface

OSPF Interface Status

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Status</th>
<th>Area ID</th>
<th>State</th>
<th>Auth-type</th>
<th>Cost</th>
<th>Priority</th>
<th>Passive</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>enabled</td>
<td>0.0.0.2</td>
<td>down</td>
<td>none</td>
<td>1</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>10.12.13.1</td>
<td>enabled</td>
<td>0.0.0.2</td>
<td>wait</td>
<td>none</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>

You can display the OSPF passive information for a particular VLAN, as shown in Example 93 (page 176).

Example 93 show ip ospf interface command for a specific VLAN with passive configured on an interface

HP Switch(config) show ip ospf interface vlan 4

OSPF configuration and statistics for VLAN 4

OSPF Interface Status for 10.10.10.1

<table>
<thead>
<tr>
<th>IP Address:</th>
<th>Status</th>
<th>AreaID</th>
<th>Passive</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>enabled</td>
<td>0.0.0.2</td>
<td>Yes</td>
</tr>
</tbody>
</table>

State : DOWN
Cost : 1
Type : BCAST
Transit Delay : 1
Hello Interval : 10
Designated Router: Events : 0
Backup Desig. Rtr: Passive : yes
Neighbors : 2

Configuring the calculation interval

Syntax:


Enables and configures SPF scheduling (throttling). This delays SPF calculations during periods of network topology changes.
SPF calculations occur at the interval set by the spf-throttle command. This command is executed in ospf context.
Default: 5 seconds

start-interval [1-600]  
Specifies the initial SPF schedule delay in seconds.
wait-interval [1-600]  
specifies the amount of time to wait until the next SPF calculation occurs, in seconds.
max-wait-time [1-600]

Specifies the maximum time between two consecutive SPF calculations, in seconds.

The current SPF interval is calculated; it will be twice as long as the previous interval until this value reaches the maximum-wait-time specified.

Example

Example 94 SPF throttling configuration

The last SPF calculation was scheduled and triggered at the 100th second. A new topology event occurred at the 104th second. The configured values are:

- start-interval = 3 seconds
- wait-interval = 3 seconds
- max-wait-time = 500 seconds

HP Switch(ospf)# spf-throttle start-interval 3 wait-interval 3 max-wait-time 500

- The difference between the last SPF (100), added to the current SPF throttle interval (3), is less than the time of the occurrence of the network event (104). SPF is scheduled to run instantly and the current SPF throttle interval is configured to 3 seconds (the start-interval value).

- Another topology event occurs within the above 3 second SPF throttle interval, at the 106th second. SPF is scheduled to run again at the 107th second (last event at 104th second + wait-interval of 3 seconds), which is greater than the current event (106th second). The SPF timer is scheduled to run after 1 second. After that, the current SPF throttle interval is changed to 10 seconds, the current wait-interval value.

- If another topology event occurs at the 110th second, which is within the 10 second current wait-time. SPF is scheduled to run again at the 117th second (last SPF of 107 seconds + wait-interval of 10 seconds), which is greater than the current event (110 seconds). The SPF timer is scheduled to run after 7 seconds. The current SPF wait-time is doubled to 20 seconds.

If any topology event occurs during the dynamic wait-interval, SPF is scheduled according to the formula:

\[
\text{Last SPF} + \text{current dynamic wait-interval} - \text{time of occurrence of the event}
\]

The dynamic wait-interval keeps doubling until the max-wait-time is reached. If the max-wait-time is reached and the network continues to be unstable, the dynamic wait-time is set to the max-wait-time until the network stabilizes.

If the network stabilizes during a dynamic wait-interval period, SPF is calculated immediately and the current SPF wait-interval is set to the configured start-interval.

Viewing OSPF information

Viewing general OSPF configuration information

Syntax:

```
show ip ospf general
```
Example

Example 95 show ip ospf general output

HP Switch(config)# show ip ospf general

OSPF General Status

OSPF protocol : enabled
Router ID : 17.255.134.231
RFC 1583 compatibility : compatible

Intra-area distance : 110
Inter-area distance : 110
AS-external distance : 110

Default import metric : 10
Default import metric type : external type 2

Area Border : no
AS Border : no
External LSA Count : 0
External LSA Checksum Sum : 0
Originate New LSA Count : 0
Receive New LSA Count : 0

Graceful Restart Interval : 120
Graceful Restart Strict-Lsa Checking : Enabled
Nonstop forwarding : Disabled

Log Neighbor Adjacency Changes : Enabled

SPF Throttling

Start Interval : 3
Wait Interval : 3
Maximum Wait Time : 500
Current Wait Interval : 3

The show running-config command also displays the SPF configuration information. The configured parameters for SPF are highlighted in bold below.

HP Switch(config)# show running-config

Running configuration:

; J8693A Configuration Editor; Created on release #K.15.07.0000x
; Ver #01:2f:2e
hostname "HP Switch"
module 1 type J86yyA
module 2 type J86xxA
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-4,7-48,A1-A4
  ipv6 address fe80::2 link-local
  ip address dhcp-bootp
  ipv6 enable
  no untagged 5-6
exit
power-over-ethernet pre-std-detect
router ospf
  spf-throttle start-interval 3 wait-interval 3 max-wait-time 500
exit
snmp-server community "public" unrestricted

The following fields are shown in the OSPF general status display:

**Table 20 CLI display of OSPF general information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF protocol</td>
<td>Whether OSPF is currently enabled.</td>
</tr>
<tr>
<td>Router ID</td>
<td>Router ID that this routing switch is currently using to identify itself</td>
</tr>
<tr>
<td>RFC 1583 compatibility</td>
<td>Whether the routing switch is currently using RFC 1583 (compatible) or</td>
</tr>
<tr>
<td></td>
<td>RFC 2328 (non-compatible rules for calculating external routes.</td>
</tr>
<tr>
<td>Intra-area distance</td>
<td>Administrative distance for routes within OSPF areas</td>
</tr>
<tr>
<td>Inter-area distance</td>
<td>Administrative distance for routes between areas within the same OSPF</td>
</tr>
<tr>
<td></td>
<td>domain</td>
</tr>
<tr>
<td>AS-external</td>
<td>Administrative distance for routes between the OSPF domain and other,</td>
</tr>
<tr>
<td></td>
<td>Exterior Gateway Protocol domains</td>
</tr>
<tr>
<td>Default import metric</td>
<td>Default metric that will be used for any routes redistributed into OSPF</td>
</tr>
<tr>
<td></td>
<td>by this routing switch</td>
</tr>
<tr>
<td>Default import metric type</td>
<td>Metric type (type 1 or type 2) that will be used for any routes</td>
</tr>
<tr>
<td></td>
<td>redistributed into OSPF by this routing switch</td>
</tr>
<tr>
<td>Area Border</td>
<td>Whether this routing switch is currently acting as an area border router</td>
</tr>
<tr>
<td>AS Border</td>
<td>Whether this routing switch is currently acting as an AS border router</td>
</tr>
<tr>
<td></td>
<td>(redistributing routes)</td>
</tr>
<tr>
<td>External LSA Count</td>
<td>Total number of external LSAs currently in the routing switch’s link</td>
</tr>
<tr>
<td></td>
<td>state database</td>
</tr>
<tr>
<td>External LSA Checksum Sum</td>
<td>Sum of the checksums of all external LSAs currently in the routing</td>
</tr>
<tr>
<td></td>
<td>switch’s link state database (quick check for whether database is in</td>
</tr>
<tr>
<td></td>
<td>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>
<tr>
<td>Graceful Restart Interval</td>
<td>Maximum seconds between graceful restarts</td>
</tr>
<tr>
<td>Graceful Restart Strict-Lsa Checking</td>
<td>Whether LSA checking is enabled or disabled (terminates</td>
</tr>
<tr>
<td></td>
<td>graceful restart when a change to an LSA would cause flooding during</td>
</tr>
<tr>
<td></td>
<td>the restart)</td>
</tr>
<tr>
<td>Nonstop forwarding</td>
<td>Whether nonstop forwarding (NSF) is enabled or disabled</td>
</tr>
<tr>
<td>Log Neighbor Adjacency Changes</td>
<td>Whether changes in adjacent neighbors are logged</td>
</tr>
</tbody>
</table>

Viewing OSPF area information

**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 information found in Table 21 (page 180):
Table 21 CLI display of OSPF area information

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area ID</td>
<td>Identifier for this area.</td>
</tr>
<tr>
<td>Type</td>
<td>Area type, which can be either &quot;normal&quot; or &quot;stub&quot;.</td>
</tr>
<tr>
<td>Cost</td>
<td>Metric for the default route that the routing switch will inject into a stub area if the routing switch is an ABR for the area. This value applies only to stub areas.</td>
</tr>
<tr>
<td>SPFR</td>
<td>Number of times the routing switch has run the shortest path first route calculation for this area.</td>
</tr>
<tr>
<td>ABR</td>
<td>Number of area border routers in this area.</td>
</tr>
<tr>
<td>ASBR</td>
<td>Number of autonomous system border routers in this area.</td>
</tr>
<tr>
<td>LSA</td>
<td>Number of LSAs in the link state database for this area.</td>
</tr>
<tr>
<td>Chksum(Hex)</td>
<td>Sum of the checksums of all LSAs currently in the area's link state database. This value can be compared to the value for other routers in the area to verify database synchronization.</td>
</tr>
</tbody>
</table>

Example

Example 96 show ip ospf area output

HP Switch(config)# show ip ospf area

OSPF Area Information

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Type</th>
<th>Cost</th>
<th>SPFR</th>
<th>ABR</th>
<th>ASBR</th>
<th>LSA</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>normal</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0x0000781f</td>
</tr>
<tr>
<td>192.147.60.0</td>
<td>normal</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0x0000fee6</td>
</tr>
<tr>
<td>192.147.80.0</td>
<td>stub</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0x000181cd</td>
</tr>
</tbody>
</table>

Viewing OSPF external link-state information

Syntax:

show ip ospf external-link-state

When you enter this command, an output similar to the following is displayed:

Example 97 Example of show ip ospf external-link-state output

HP Switch# show ip ospf external-link-state

OSPF External LSAs

<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>0x0000d99f</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>0x800009cd</td>
<td>0x0000b9dd</td>
</tr>
</tbody>
</table>

Table 22 (page 181) shows the information the OSPF external link state displays:
Table 22 CLI display of OSPF external link state information

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link State ID</td>
<td>LSA ID for this LSA. Normally, the destination of the external route,</td>
</tr>
<tr>
<td></td>
<td>but may have some &quot;host&quot; 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] [subset-options]
router-id  ip-addr
```

Subset option to filter displayed external-link-state data to show LSAs with the specified router ID only. Can also be filtered by using the link-state-id or sequence-number options.

```
sequence-number  integer
```

Subset option to filter displayed external-link-state data to show LSAs with the specified sequence number. Can also be filtered by using the link-state-id or router-id options.

```
link-state-id  ip-addr
```

Subset option to filter displayed external-link-state data to show LSAs with the specified ID only. Can also be filtered by using the sequence-number or router-id options.

Syntax:

```
show ip ospf external-link-state [status] advertise
```

Displays the hexadecimal data in the specified LSA packet, the actual contents of the LSAs. Can also be filtered by using the link-state-id, router-id, or sequence-number options.

Example

**Example 98 Output for show ip ospf external-link-state advertise**

```
HP Switch# show ip ospf external-link-state advertise

OSPF External LSAs
Advertisements
------------------------------------------------------------------------
000302050a0307000a00082580000005d99f0024fffffff008000000a0000000000000000
000302050a0308000a00082580000005cea90024fffffff008000000a0000000000000000
000302050a0309000a00082580000005c3b30024fffffff008000000a0000000000000000
000302050a030a000a00082580000005b8bd0024fffffff008000000a0000000000000000
000002050a0321000a000824800009cdb9dd0024fffffff00800000010000000000000000
```

Viewing OSPF interface information

Syntax:

```
show ip ospf interface [ vlan vlan-id | ip-addr ]
```
**ip-address**
Displays the OSPF interface information for the specified IP address.

**vlan-id**
Displays the OSPF interface information for the specified IP address.

Table 23 (page 182) shows the information displayed for the OSPF interface.

**Table 23 CLI display of OSPF interface information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</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>
<tr>
<td>State</td>
<td>The current state of the interface. The value will be one of the following:</td>
</tr>
<tr>
<td></td>
<td>DOWN—The underlying VLAN is down.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>DR—This switch is the designated router for this interface.</td>
</tr>
<tr>
<td></td>
<td>BDR—This switch is the backup designated router for this interface.</td>
</tr>
<tr>
<td></td>
<td>DROTHER—This router is not the designated router or backup designated router for this interface.</td>
</tr>
<tr>
<td>Auth-type</td>
<td>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.</td>
</tr>
<tr>
<td>Chain</td>
<td>The name of the key chain configured for the specified interface. (See chapter “Key Management System” in the Access Security Guide for your routing switch.</td>
</tr>
<tr>
<td>Cost</td>
<td>The OSPF’s metric for this interface.</td>
</tr>
<tr>
<td>Pri</td>
<td>This routing switch’s priority on this interface for use in the designated router election algorithm.</td>
</tr>
<tr>
<td>Passive</td>
<td>Whether the interface sends link-state advertisements (LSAs) to all other routers in the same Autonomous System (AS).</td>
</tr>
</tbody>
</table>

**Example**

**Example 99 Output for show ip ospf interface**

```
HP Switch# show ip ospf interface

OSPF Interface Status

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Status</th>
<th>Area ID</th>
<th>State</th>
<th>Auth-type</th>
<th>Cost</th>
<th>Pri</th>
<th>Passive</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.18.36</td>
<td>enabled</td>
<td>10.3.16.0</td>
<td>DOWN</td>
<td>none</td>
<td>1</td>
<td>1</td>
<td>no</td>
</tr>
<tr>
<td>10.3.53.36</td>
<td>enabled</td>
<td>10.3.48.0</td>
<td>BDR</td>
<td>none</td>
<td>1</td>
<td>1</td>
<td>no</td>
</tr>
</tbody>
</table>
```

**Viewing OSPF interface information for a specific VLAN or IP address**

**Syntax:**

```
show ip ospf interface [ vlan vlan-id | ip-addr ]
```
To display OSPF interface information for a specific VLAN or IP address, enter the `show ip ospf interface ip-addr` command at any CLI level.

### Table 24 CLI display of OSPF interface information—VLAN or IP address

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Will always be BCAST for interfaces on this routing switch. Point-to-point or NBMA (frame relay or ATM) type interfaces are not supported on the 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 DR on this interface.</td>
</tr>
<tr>
<td>Backup Desig. Rtr</td>
<td>IP address of the router that has been elected BDR on this interface.</td>
</tr>
<tr>
<td>Events</td>
<td>Number of times the interface state has changed.</td>
</tr>
<tr>
<td>Passive</td>
<td>Whether the interface sends LSAs to all other routers in the same Autonomous System (AS).</td>
</tr>
<tr>
<td>Neighbors</td>
<td>Number of neighbors.</td>
</tr>
</tbody>
</table>

If you use `show ip ospf interface vlan vlan-id`, the output is the same as shown in the previous table, except for the IP address on the indicated VLAN.

**Example**

**Example 100 show ip ospf interface ip-addr output**

```
HP Switch(ospf)# sho ip ospf int 10.10.50.1

OSPF Interface Status for 10.3.1836

    IP Address     : 10.3.18.36          Status : enabled
    Area ID        : 10.3.16.0

    State : BDR                             Auth-type : none
    Cost  : 1                                Chain :
    Type  : BCAST                           Priority : 1

    Transit Delay : 1                        Retrans Interval : 5
    Hello Interval : 10                       Rtr Dead Interval : 40
    Designated Router : 10.3.18.34          Events : 3
    Backup Desig. Rtr : 10.3.18.36           Backup Desig. Rtr : 10.3.18.36
```

**Viewing OSPF packet statistics for a subnet or VLAN**

Displays the statistics on OSPF packets sent and received on the interfaces in VLANs and/or subnets on an OSPF-enabled routing switch, including the number of errors that occurred during packet transmission. Enter the command at any CLI level.

**Syntax:**

```
show ip ospf interface [[vlan vlan-id] | ip-address]
```

Displays the following information for OSPF-enabled VLANs and/or subnets:
**Example 101 Displaying OSPF statistics for VLAN traffic**

HP Switch(ospf)# show ip ospf statistics vlan 1

OSPF statistics for VLAN 1

OSPF Interface Status for 10.0.0.2

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tx Hello Packet Count</td>
<td>16</td>
</tr>
<tr>
<td>Rx Hello Packet Count</td>
<td>16</td>
</tr>
<tr>
<td>Tx DD Packet Count</td>
<td>2</td>
</tr>
<tr>
<td>Rx DD Packet Count</td>
<td>4</td>
</tr>
<tr>
<td>Tx LSR Packet Count</td>
<td>1</td>
</tr>
<tr>
<td>Rx LSR Packet Count</td>
<td>1</td>
</tr>
<tr>
<td>Tx LSU Packet Count</td>
<td>5</td>
</tr>
<tr>
<td>Rx LSU Packet Count</td>
<td>2</td>
</tr>
<tr>
<td>Tx LSA Packet Count</td>
<td>2</td>
</tr>
<tr>
<td>Rx LSA Packet Count</td>
<td>3</td>
</tr>
</tbody>
</table>

OSPF Errors: 26

**Table 25 CLI display of OSPF statistics for VLAN traffic**

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF statistics for VLAN</td>
<td>OSPF statistics displayed for the specified VLAN number.</td>
</tr>
<tr>
<td>vlan-id</td>
<td></td>
</tr>
<tr>
<td>OSPF Interface Status for</td>
<td>IP address of a subnet on the VLAN.</td>
</tr>
<tr>
<td>ip-address</td>
<td></td>
</tr>
<tr>
<td>Tx/Rx Hello Packet Count</td>
<td>Number of OSPF hello packets sent/received on each subnet interface.</td>
</tr>
<tr>
<td>Tx/Rx DD Packet Count</td>
<td>Number of link-state database description packets sent/received on each subnet interface.</td>
</tr>
<tr>
<td>Tx/Rx LSR Packet Count</td>
<td>Number of link-state request packets sent/received on each subnet interface.</td>
</tr>
<tr>
<td>Tx/Rx LSU Packet Count</td>
<td>Number of link-state update packets sent/received on each subnet interface.</td>
</tr>
<tr>
<td>Tx/Rx LSA Packet Count</td>
<td>Number of link-state acknowledgement packets sent/received on each subnet interface.</td>
</tr>
<tr>
<td>OSPF errors</td>
<td>Number of errors detected on the VLAN subnet during OSPF packet exchange.</td>
</tr>
</tbody>
</table>
Example 102 Displaying OSPF statistics for subnet traffic

HP Switch(ospf)# show ip ospf statistics 10.0.0.2

OSPF Interface Statistics

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Total Tx</th>
<th>Total Rx</th>
<th>Total Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.2</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
</tbody>
</table>

Table 26 CLI display of OSPF statistics for VLAN subnet traffic

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address of subnet.</td>
</tr>
<tr>
<td>Total Tx</td>
<td>Total number of OSPF packets sent on each subnet interface.</td>
</tr>
<tr>
<td>Total Rx</td>
<td>Total number of OSPF packets received on each subnet interface.</td>
</tr>
<tr>
<td>Total Errors</td>
<td>Total number of errors in OSPF packet transmission on each subnet interface.</td>
</tr>
</tbody>
</table>

Clearing OSPF statistics for all VLAN interfaces on the switch

**Syntax:**

clear ip ospf statistics

Clears the OSPF statistics for all VLAN interfaces on the switch and sets all VLAN/subnet counters for OSPF traffic to zero. Enter the command at any CLI level.

Viewing OSPF link-state information

**Syntax:**

show ip ospf link-state [status] [subsetoptions] [advertise [subset-options]][detail]

To display OSPF link state information, enter `show ip ospf link-state` at any CLI level.

advertise

Displays the hexadecimal data in LSA packets (advertisements) for the OSPF areas configured on the routing switch.

The output can also be filtered by area (`area-id`), link-state-id, router-id, sequence-number, and/or type.

Default: All OSPF areas configured on the routing switch.

**ospf-area-id**

Used to restrict display of LSA database or advertisements to show only the data from a specific OSPF area.

Can also be used with other subset options (`router-id, sequence-number, external link-state-id, and/or type`) to further define the source of displayed information.

**link-state-id ip-addr**

Used to restrict display of LSA database or advertisements to show only the data from sources having the specified IP address as a link-state ID.
Can also be used with other subset options \((\text{ospf-area-id}, \text{router-id}, \text{sequence-number}, \text{external link-state-id}, \text{and type})\) to further define the source of displayed information.

**router-id ip-addr**

Used to restrict display of LSA database or advertisements to show only the data from sources having the specified router ID.

Can also be used with other subset options \((\text{ospf-area-id}, \text{link-state-id}, \text{sequence-number}, \text{and type})\) to further define the source of displayed information.

**sequence-number integer**

Used to restrict display of LSA database or advertisements to show only the data from sources having the specified sequence number.

Can also be used with other subset options \((\text{ospf-area-id}, \text{link-state-id}, \text{router-id}, \text{and type})\) to further define the source of displayed information.

**type [ router | network | summary | as-summary | external | multicast | nssa ]**

Used to restrict display of LSA database or advertisements to show only the data from sources having the specified type.

Can also be used with other subset options \((\text{ospf-area-id}, \text{link-state-id}, \text{router-id}, \text{and sequence-number})\) to further define the source of displayed information.

**detail**

Displays LSA details for the OSPF area(s) configured on the routing switch. The output can also be filtered by area \((\text{area-id})\), link-state-id, router-id, and sequence-number. Default: All OSPF areas configured on the routing switch.

**Example**

When you enter this command, the switch displays an output similar to the following for all configured areas:
Example 103 show ip ospf link-state output

OSPF Link State Database for Area 0.0.0.0

<table>
<thead>
<tr>
<th>LSA Type</th>
<th>Link State ID</th>
<th>Advertising Router ID</th>
<th>Age</th>
<th>Sequence #</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.0.8.32</td>
<td>10.0.8.32</td>
<td>65</td>
<td>0x80000281</td>
<td>0x0000a7b6</td>
</tr>
<tr>
<td>Router</td>
<td>10.0.8.33</td>
<td>10.0.8.33</td>
<td>1638</td>
<td>0x80000005</td>
<td>0x0000a7c8</td>
</tr>
<tr>
<td>Network</td>
<td>10.3.2.37</td>
<td>10.0.8.37</td>
<td>1695</td>
<td>0x80000006</td>
<td>0x00000443</td>
</tr>
<tr>
<td>Summary</td>
<td>10.3.16.0</td>
<td>10.0.8.33</td>
<td>1638</td>
<td>0x80000007</td>
<td>0x0000c242</td>
</tr>
<tr>
<td>Summary</td>
<td>10.3.16.0</td>
<td>10.0.8.35</td>
<td>1316</td>
<td>0x80000008</td>
<td>0x0000aa58</td>
</tr>
<tr>
<td>Summary</td>
<td>10.3.17.0</td>
<td>10.0.8.33</td>
<td>1638</td>
<td>0x8000027b</td>
<td>0x0000becf</td>
</tr>
<tr>
<td>Summary</td>
<td>10.3.17.0</td>
<td>10.0.8.35</td>
<td>1316</td>
<td>0x80000008</td>
<td>0x0000a957</td>
</tr>
<tr>
<td>AsbSummary</td>
<td>10.0.8.36</td>
<td>10.0.8.33</td>
<td>1412</td>
<td>0x80000002</td>
<td>0x00002cba</td>
</tr>
</tbody>
</table>

OSPF Link State Database for Area 10.3.16.0

<table>
<thead>
<tr>
<th>LSA Type</th>
<th>Link State ID</th>
<th>Advertising Router ID</th>
<th>Age</th>
<th>Sequence #</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>10.0.8.33</td>
<td>10.0.8.33</td>
<td>1727</td>
<td>0x8000027e</td>
<td>0x0000d53c</td>
</tr>
<tr>
<td>Router</td>
<td>10.0.8.34</td>
<td>10.0.8.34</td>
<td>1420</td>
<td>0x80000283</td>
<td>0x0000de4f</td>
</tr>
<tr>
<td>Network</td>
<td>10.3.16.34</td>
<td>10.0.8.34</td>
<td>1735</td>
<td>0x80000005</td>
<td>0x00001465</td>
</tr>
</tbody>
</table>

The OSPF link-state display shows the following contents of the LSA database; one table for each area:

Table 27 CLI display of OSPF link-state information

<table>
<thead>
<tr>
<th>Field</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSA Type</td>
<td>The possible types are:</td>
</tr>
<tr>
<td></td>
<td>• Router</td>
</tr>
<tr>
<td></td>
<td>• Network</td>
</tr>
<tr>
<td></td>
<td>• Summary</td>
</tr>
<tr>
<td></td>
<td>• 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>
**Example 104 Output for show ip ospf link-state advertise**

HP Switch(config)# show ip ospf link-state advertise

OSPF Link State Database for Area 0.0.0.0

Advertisements

<table>
<thead>
<tr>
<th>Advertisements</th>
</tr>
</thead>
<tbody>
<tr>
<td>000202010a0008200a00082080000281a7b60054000000050a030e00fffff0003000001...</td>
</tr>
<tr>
<td>000202010a0008210a00082180000006a5c9002401000010a0008230a03112104000002</td>
</tr>
<tr>
<td>000102010a0008230a00082380000015755d06c01000070a030600fffff0003000001...</td>
</tr>
<tr>
<td>000202020a0302250a00082580000070244024fffff00a0008250a0008230a000820</td>
</tr>
<tr>
<td>000202030a0008240a000824800000032ab010c00000000000b00</td>
</tr>
<tr>
<td>000102040a0008240a00082380000004c12a001c00000000000002</td>
</tr>
</tbody>
</table>

OSPF Link State Database for Area 10.3.16.0

Advertisements

<table>
<thead>
<tr>
<th>Advertisements</th>
</tr>
</thead>
<tbody>
<tr>
<td>000202010a0008210a000821800000027fd33d0054050000050a031900fffff0003000001...</td>
</tr>
<tr>
<td>000102010a0008220a00082280000284dc50006000000060a031500fffff0003000001...</td>
</tr>
<tr>
<td>000102020a0311220a0008228000027bf908020fffff000a0008220a000821</td>
</tr>
</tbody>
</table>

**Example 105 Output for show IP OSPF link-state detail for router**

This is an example of show ip ospf link-state detail output for a router.

HP Switch(config)# show ip ospf link-state detail

OSPF Link State Database for Area 0.0.0.0

| LSA Age | : 35 |
| LSA Type | : 0x1 (Router) |
| Advertising Router | : 2.2.2.3 |
| Link State ID | : 2.2.2.3 |
| LSA Sequence | : 0x80000007 |
| LSA Checksum | : 0xfd09 |
| LSA Option Bits | : E=1 MC=0 N/P=0 EA=0 DC=1 |
| Router Capability Bits | : B=0 E=1 V=0 |
| Number of links | : 1 |
| Interface Type | : 2 (Connected to Transit Network) |
| LSA Metric | : 1 |
| Link Data | : 2.2.2.3 |
| LSA ID | : 2.2.2.3 |
| Number of TOS Metrics | : 0 |
Example 106 Output for show IP OSPF link-state detail for a network

This is an example of `show ip ospf link-state detail` summary for LSA detailed output.

HP Switch(config)# show ip ospf link-state detail

OSPF Link State Database for Area 0.0.0.0

| LSA Age | : 19 |
| LSA Type | : 0x2 (Network) |
| Advertising Router | : 16.93.223.84 |
| Link State ID | : 192.22.23.24 |
| LSA Sequence | : 0x80000001 |
| LSA Checksum | : 0x323e |
| LSA Option Bits | : E=1 MC=0 N/P=0 EA=0 DC=1 |
| Network Mask | : 255.255.255.0 |
| Attached Router ID | : 2.2.2.3 |
| Attached Router ID | : 192.93.226.105 |

Example 107 Output for show IP OSPF link-state detail for summary of LSA detailed output

This is an example of `show ip ospf link-state detail` summary of LSA for AS Boundary Router.

HP Switch(config)# show ip ospf link-state detail

OSPF Link State Database for Area 0.0.0.0

| LSA Age | : 58 |
| LSA Type | : 0x4 (AS Boundary) |
| Advertising Router | : 16.93.226.105 |
| Link State ID | : 2.2.2.3 |
| LSA Sequence | : 0x80000001 |
| LSA Checksum | : 0x4bc4 |
| LSA Option Bits | : E=1 MC=0 N/P=0 EA=0 DC=1 |
| LSA Metric | : 1 |

Example 108 Output for show IP OSPF link-state detail for AS external LSA

This example shows `show ip ospf link-state detail` for an AS external LSA.

HP Switch(config)# show ip ospf link-state detail

OSPF Link State Database for Area 0.0.0.0

| LSA Age | : 971 |
| LSA Type | : 0x5 (AS External) |
| Advertising Router | : 2.2.2.3 |
| Link State ID | : 55.5.5.0 |
| LSA Sequence | : 0x80000001 |
| LSA Checksum | : 0xe17c |
| LSA Option Bits | : E=1 MC=0 N/P=0 EA=0 DC=0 |
| LSA Metric | : 10 |
| Bit E | : 0 |
| Forwarding Address | : 0.0.0.0 |
Example 109 Output for show IP OSPF link-state detail for summary for NSSA

This example shows show ip ospf link-state detail summary for NSSA.

HP Switch(config)# show ip ospf link-state detail

| LSA Age  | : 86 |
| LSA Type | : 0x7 (NSSA) |
| Advertising Router | : 16.93.226.105 |
| Link State ID | : 16.93.49.0 |
| LSA Sequence | : 0x80000003 |
| LSA Checksum | : 0x6c03 |
| LSA Option Bits | : E=1 MC=0 N/P=0 EA=0 DC=1 |
| LSA Metric | : 10 |
| Network Mask | : 255.255.255.0 |
| Bit E | : 0 (External Metric Type1) |
| Forwarding Address | : 0.0.0.0 |
| External Route Tag | : 0 |

Viewing OSPF neighbor information

Syntax:

```
show ip ospf neighbor [ ip-addr]
```

To display OSPF information for all neighbors, enter show ip ospf neighbor at any CLI level.

[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.

Example

Example 110 show ip ospf neighbor output

OSPF Neighbor Information

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Pri</th>
<th>IP Address</th>
<th>NbIfState</th>
<th>State</th>
<th>Rxmt</th>
<th>QLen</th>
<th>Events</th>
<th>Helper Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.8.34</td>
<td>1</td>
<td>10.3.18.34</td>
<td>DR</td>
<td>FULL</td>
<td>0</td>
<td>6</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>10.3.53.38</td>
<td>1</td>
<td>10.3.53.38</td>
<td>DR</td>
<td>FULL</td>
<td>0</td>
<td>6</td>
<td>none</td>
<td></td>
</tr>
</tbody>
</table>

This display shows the following information.

Table 28 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 DR and 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>
</tbody>
</table>

190 Open Shortest Path First Protocol (OSPF)
Table 28 CLI display of OSPF neighbor information  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>The state of the conversation (the adjacency) between your routing switch and the neighbor. The possible values are:</td>
</tr>
</tbody>
</table>
|             | INIT  
|             | A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor. (The 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. |
|             | 2WAY  
|             | Communication between the two routers is bidirectional. This is the most advanced state before beginning adjacency establishment. The DR and BDR are selected from the set of neighbors in the 2Way state or greater. |
|             | 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. |
|             | EXCHANGE  
|             | The switch is describing its entire link state database by sending DD packets to the neighbor. Each DD packet has a DD sequence number and is explicitly acknowledged. Only one DD 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. |
|             | 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. |
|             | FULL  
|             | The neighboring routers are fully adjacent. These adjacencies will now appear in router links and network link advertisements. |
| Rxmt QLen   | 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. |
| Events      | The number of times the neighbor’s state has changed. |
| Helper Status | Whether the neighboring router is helping the OSPF router. The possible values are: |
|             | Helper  
|             | The neighbor is helping. |
|             | None  
|             | The neighbor is not helping. |
| Helper Age  | Amount of time the neighboring router is helping. This time can range from 1 to 1800 seconds with a default time of 120 seconds. Helper Age is 0 when the router is not helping. |

**Viewing OSPF redistribution information**

As described under “Enabling route redistribution” (page 161), you can configure the routing switch to redistribute connected, static, and RIP 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 `show ip ospf redistribute` at any CLI context level:
Example 111 Example of output for show ip ospf redistribute

HP Switch# show ip ospf redistribute

OSPF redistributing
Route type Status
------------- --------
connected enabled
static enabled
rip enabled

The display shows whether redistribution of each of the route types, connected, static, and RIP is enabled.

Viewing OSPF redistribution filter (restrict) information

As described under “Configuring external route redistribution in an OSPF domain (optional)” (page 160), 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 show ip ospf restrict at any CLI context level.

Example 112 Example of output for show ip ospf restrict

HP Switch# show ip ospf restrict

OSPF restrict list

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.8.0</td>
<td>255.255.248.0</td>
</tr>
<tr>
<td>15.0.0.0</td>
<td>255.0.0.0</td>
</tr>
</tbody>
</table>

This display shows the configured restrict entries.

Viewing OSPF virtual neighbor information

If virtual links are configured on the routing switch, you can display OSPF virtual neighbor information.

Syntax:

    show ip ospf virtual-neighbor [[area area-id] | [ip-address]]

Example 113 Example of output for show ip ospf virtual-neighbor

OSPF Virtual Interface Neighbor Information

<table>
<thead>
<tr>
<th>Router ID</th>
<th>Area ID</th>
<th>State</th>
<th>IP Address</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.8.33</td>
<td>10.3.16.0</td>
<td>FULL</td>
<td>10.3.17.33</td>
<td>5</td>
</tr>
<tr>
<td>10.0.8.36</td>
<td>10.3.16.0</td>
<td>FULL</td>
<td>10.3.18.36</td>
<td>5</td>
</tr>
</tbody>
</table>

This display shows the following information.

Table 29 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>
</tbody>
</table>
Table 29 CLI display of OSPF virtual neighbor information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 “CLI display of OSPF neighbor information” (page 190). 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 `ip-address` can be specified to display detailed information for a particular virtual neighbor. If an `area-id` is specified, only virtual neighbors belonging to that area are shown.

Viewing OSPF virtual link information

**Syntax:**

```
show ip ospf virtual-link [area area-id] | [ip-address]
```

- `ip-address` Displays detailed information for a particular virtual neighbor.
- `area-id` Only virtual neighbors belonging to that area are shown.

**Example 114 Example of output for show ip ospf virtual-link**

If virtual links are configured on a routing switch, you can display OSPF virtual link information by entering `show ip ospf virtual-link` at any CLI level.

HP Switch# show ip ospf virtual-link

**OSPF Virtual Interface Status**

<table>
<thead>
<tr>
<th>Transit Area ID</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>

This display shows the following information.

Table 30 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: DOWN The routing switch has not yet found a route to the virtual neighbor. P2P (point-to-point) The routing switch has found a route to the virtual neighbor. Virtual links are &quot;virtual&quot; serial links, hence the point-to-point terminology.</td>
</tr>
</tbody>
</table>

Notice from the syntax statement that `ip-address` can be specified to display detailed information for a particular virtual neighbor. If an `area-id` is specified, only virtual neighbors belonging to that area are shown.
Example
To get OSPF virtual link information for IP address 10.0.8.33, enter `show ip ospf virtual-link 10.0.8.33`. A display similar to the following is shown.

**Example 115 Output for show ip ospf virtual-link ip-addr**

```
HP Switch# show ip ospf virtual-link 10.0.8.33

OSPF Virtual Interface Status for interface 10.0.8.33
  Transit AreaID : 10.3.16.0
  Neighbor Router : 10.0.8.33

  Authentication : none
  Interface State : P2P
  Events          : 1
  Dead Interval   : 40

Chain          : 
  Transit Delay : 1
  Rtr Interval  : 5
  Hello Interval: 10
```

In this display, these fields show the same type of information as described for the general OSPF virtual link display: Transit Area ID, Neighbor Router, Authentication, and Interface State. This display shows the following additional information:

**Table 31 CLI display of OSPF virtual link information—Specific IP address**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>The number of times the virtual link interface state has changed.</td>
</tr>
<tr>
<td>Transit delay</td>
<td>The configured transit delay for the virtual link.</td>
</tr>
<tr>
<td>Rtr Interval</td>
<td>The configured retransmit interval for the virtual link.</td>
</tr>
<tr>
<td>Hello Interval</td>
<td>The configured hello interval for the virtual link.</td>
</tr>
<tr>
<td>Dead Interval</td>
<td>The configured router dead interval for the virtual link.</td>
</tr>
</tbody>
</table>

**Viewing OSPF SPF statistics**

Displays the log used to record SPF calculations on an OSPF-enabled routing switch. The SPF algorithm recalculates the routes in an OSPF domain when a change in the area topology is received.

**Syntax:**

```
show ip ospf spf-log
```

This command output displays:

- The number of times that the SPF algorithm was executed for each OSPF area to which the routing switch is assigned.
- The event that resulted in the last ten executions of the SPF algorithm on the routing switch. Possible events (reasons) are as follows:
  - Re-init
    - OSPF was enabled or disabled on the routing switch.
  - Router LS update
    - A router (type 1) link-state advertisement was received.
  - Network LS update
    - A network (type 2) link-state advertisement was received.
  - Generated RTR LSA
    - A router (type 1) link-state advertisement was generated on the routing switch.
Generated NTW LSA
A network (type 2) link-state advertisement was generated on the routing switch.

Example 116 Displaying OSPF SPF statistics

HP Switch(ospf)# show ip ospf spf-log

OSPF SPF (SHORTEST PATH FIRST) LOG

Area : 0.0.0.100 - Number of times SPF executed : 12

<table>
<thead>
<tr>
<th>SPF Instance</th>
<th>Reason</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Router LS Update</td>
<td>0h:35m:44</td>
</tr>
<tr>
<td>2</td>
<td>Router LS Update</td>
<td>0h:36m:03</td>
</tr>
<tr>
<td>3</td>
<td>Generated RTR LSA</td>
<td>1h:04m:21</td>
</tr>
<tr>
<td>4</td>
<td>Generated NTW LSA</td>
<td>1h:28m:12</td>
</tr>
<tr>
<td>5</td>
<td>Network LS Update</td>
<td>2h:11m:05</td>
</tr>
<tr>
<td>6</td>
<td>Network LS Update</td>
<td>2h:54m:55</td>
</tr>
<tr>
<td>7</td>
<td>Generated RTR LSA</td>
<td>3h:01m:11</td>
</tr>
<tr>
<td>8</td>
<td>Router LS Update</td>
<td>3h:22m:39</td>
</tr>
<tr>
<td>9</td>
<td>Generated RTR LSA</td>
<td>4h:36m:22</td>
</tr>
<tr>
<td>10</td>
<td>Re-Init</td>
<td>4h:48m:54</td>
</tr>
</tbody>
</table>

Table 32 CLI display of OSPF SPF statistics

<table>
<thead>
<tr>
<th>area [area id</th>
<th>ip-address]</th>
<th>ID number or IP address of an area to which the switch is assigned, including the number of times the SPF algorithm was executed to recalculate OSPF routes in the area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPF instances</td>
<td></td>
<td>Last ten instances in which the SPF algorithm was executed to recalculate an OSPF route in the area.</td>
</tr>
<tr>
<td>Reason</td>
<td></td>
<td>The event or reason why the SPF algorithm was executed.</td>
</tr>
<tr>
<td>Time</td>
<td></td>
<td>Time when the SPF computation began.</td>
</tr>
</tbody>
</table>

Displaying OSPF route information

Syntax:

show ip ospf

To display OSPF route and other OSPF configuration information, enter `show ip ospf` at any CLI level.
Example 117 Output for show IP OSPF

HP Switch# show ip ospf

OSPF Configuration Information

- OSPF protocol: enabled
- Router ID: 10.0.8.35

Current defined areas:

<table>
<thead>
<tr>
<th>Area ID</th>
<th>Type</th>
<th>Default Cost</th>
<th>Summary LSA</th>
<th>Metric Type</th>
<th>SPF Runs</th>
</tr>
</thead>
<tbody>
<tr>
<td>backbone</td>
<td>normal</td>
<td>1</td>
<td>don't send</td>
<td>ospf metric 1</td>
<td></td>
</tr>
<tr>
<td>10.3.16.0</td>
<td>normal</td>
<td>1</td>
<td>don't send</td>
<td>ospf metric 1</td>
<td></td>
</tr>
<tr>
<td>10.3.32.0</td>
<td>normal</td>
<td>1</td>
<td>don't send</td>
<td>ospf metric 1</td>
<td></td>
</tr>
</tbody>
</table>

Current defined address ranges:

<table>
<thead>
<tr>
<th>Area ID</th>
<th>LSA Type</th>
<th>IP Network</th>
<th>Network Mask</th>
<th>Advertise Cost</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 1</td>
</tr>
</tbody>
</table>

OSPF interface configuration:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Area ID</th>
<th>Status</th>
<th>Type</th>
<th>Authen Xmit</th>
<th>Rxmt</th>
<th>Hello Delay</th>
<th>Intvl</th>
<th>Dead Delay</th>
<th>Intvl</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>
<td>10</td>
<td>40</td>
<td>10</td>
<td>40</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>
<td>10</td>
<td>40</td>
<td>10</td>
<td>40</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>
<td>10</td>
<td>40</td>
<td>10</td>
<td>40</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>
<td>10</td>
<td>40</td>
<td>10</td>
<td>40</td>
</tr>
</tbody>
</table>

OSPF configured interface timers:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Transit Delay</th>
<th>Retransmit Delay</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 Delay</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>

Table 33 CLI display of OSPF route and status information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF protocol</td>
<td>enabled or disabled — 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>
<tr>
<td>Currently defined areas:</td>
<td></td>
</tr>
<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>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Stub Default Cost</td>
<td>The metric for any default route we injected into a stub area if the routing switch is an ABR for the area. This value applies only to stub areas.</td>
</tr>
<tr>
<td>Stub Summary LSA</td>
<td>send or don’t send — 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). Applies only to stub areas and takes effect only if the routing switch is the ABR for the area.</td>
</tr>
<tr>
<td>Stub Metric Type</td>
<td>This value is always ospf metric.</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 Summary.</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 advertising (yes) or suppressing (no) this address range.</td>
</tr>
<tr>
<td>Cost</td>
<td>The cost of the interface connection between one switch and another, which is determined by the bandwidth in mega bits per second. The OSPF protocol determines the interface connection cost of each neighbor and uses these costs to determine the best path to reach a destination. The cost can range from a minimum of 1 to a maximum of 10. The faster the connection, the lower the cost. For example, a fast Ethernet interface cost is 1 and a Ethernet interface cost is 10.</td>
</tr>
</tbody>
</table>

**NOTE:** The remaining interface and virtual link information is the same as for the previously described OSPF show commands. See Table 23 (page 182) and Table 24 (page 183).

**Viewing OSPF traps enabled**

In the default configuration, OSPF traps are disabled. Use this command to view which OSPF traps have been enabled.

**Syntax:**

```bash
show ip ospf traps
```

Lists the OSPF traps currently enabled on the routing switch.

For more information on OSPF trap use, See “Changing OSPF trap generation choices (optional)” (page 165).

**Debugging OSPF routing messages**

**Syntax:**

```bash
debug ip ospf
```

Turns on the tracing of OSPF packets and displays OSPF routing messages.

**Enabling load sharing among next-hop routes**

For more information, see “OSPF equal-cost multipath (ECMP) for different subnets available through the same next-hop routes” (page 213).

**Syntax:**

```bash
[no] ip load-sharing 2-4
```

Enabling load sharing among next-hop routes 197
When OSPF is enabled and multiple, equal-cost, next-hop routes are available for traffic destinations on different subnets, this feature, by default, enables load-sharing among up to four next-hop routes.

1 - 4 : Specifies the maximum number of equal-cost next-hop paths the router allows.

Default: 4; range: 2–4

The no form of the command disables this load-sharing so that only one route in a group of multiple, equal-cost, next-hop routes is used for traffic that could otherwise be load-shared across multiple routes.

For example, in Figure 35 (page 213), the next-hop routers "B", "C", and "D" are available for equal-cost load-sharing of eligible traffic. Disabling IP load-sharing means that router "A" selects only one next-hop router for traffic that is actually eligible for load-sharing through different next-hop routers.

Default: Enabled with four equal-cost, next-hop routes allowed

NOTE: This command enables or disables load-sharing for both IPv4 (OSPFv2) and IPv6 (OSPFv3) operation. For more information on load-sharing, see the latest IPv6 Configuration Guide for your routing switch.

In the default configuration, IP load-sharing is enabled by default. However, it has no effect unless IP routing and OSPF are enabled.

Viewing the current IP load-sharing configuration

Use the show running command to view the currently active IP load-sharing configuration, and show config to view the IP load-sharing configuration in the startup-config file. (While in its default configuration, IP load-sharing does not appear in the command output.)

If IP load sharing is configured with non-default settings (disabled or configured for either two or three equal-cost next-hop paths), the current settings are displayed in the command output.

Figure 28 Displaying a non-default IP load-sharing configuration

Overview of OSPF

OSPF is a link-state routing protocol applied to routers grouped into OSPF areas identified by the routing configuration on each routing switch. The protocol uses LSAs transmitted by each router to update neighboring routers regarding its interfaces and the routes available through those interfaces. Each routing switch in an area also maintains a link-state database (LSDB) that describes the area topology. (All routers in a given OSPF area have identical LSDBs.) The routing switches used to connect areas to each other flood summary link LSAs and external link LSAs to neighboring OSPF areas to update them regarding available routes. Through this means, each OSPF router determines
the shortest path between itself and a desired destination router in the same OSPF domain (AS). Routed traffic in an OSPF AS is classified as one of the following:

- Intra-area traffic
- Inter-area traffic
- External traffic

The switches support the following types of LSAs, which are described in RFCs 2328 and 3101:

**Table 34 OSPF LSA types**

<table>
<thead>
<tr>
<th>LSA type</th>
<th>LSA name</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Router link</td>
<td>Describes the state of each interface on a router for a given area. Not propagated to backbone area.</td>
</tr>
<tr>
<td>2</td>
<td>Network link</td>
<td>Describes the OSPF routers in a given network. Not propagated to backbone area.</td>
</tr>
<tr>
<td>3</td>
<td>Summary link</td>
<td>Describes the route to networks in another OSPF area of the same AS. Propagated through backbone area to other areas.</td>
</tr>
<tr>
<td>4</td>
<td>Autonomous System (AS) summary link</td>
<td>Describes the route to an ASBR in an OSPF normal or backbone area of the same AS. Propagated through backbone area to other areas.</td>
</tr>
<tr>
<td>5</td>
<td>AS external link</td>
<td>Describes the route to a destination in another AS (external route). Originated by ASBR in normal or backbone areas of an AS and propagates through backbone area to other normal areas. For injection into an NSSA, ABR converts type-5 LSAs to a type-7 LSA advertising the default route (0.0.0.0/0).</td>
</tr>
<tr>
<td>7</td>
<td>AS external link in an NSSA</td>
<td>Describes the route to a destination in another AS (external route). Originated by ASBR in NSSA. ABR converts type-7 LSAs to type-5 LSAs for injection into the backbone area.</td>
</tr>
</tbody>
</table>

**OSPF router types**

**Interior routers**

This type of OSPF router belongs to only one area. Interior routers flood type-1 LSAs to all routers in the same area and maintain identical LSDBs. In Figure 29 (page 199), routers R1, R3, R4, and R6 are all interior routers because all of their links are to other routers in the same area.

**Figure 29 Example of interior routers**
Area border routers (ABRs)

This type of OSPF router has membership in multiple areas. ABRs are used to connect the various areas in an AS to the backbone area for that AS. Multiple ABRs can be used to connect a given area to the backbone, and a given ABR can belong to multiple areas other than the backbone.

An ABR maintains a separate LSDB for each area to which it belongs. (All routers within the same area have identical LSDBs.) The ABR is responsible for flooding summary LSAs between its border areas. You can reduce summary LSA flooding by configuring area ranges. An area range enables you to assign an aggregate address to a range of IP addresses. This aggregate address is advertised instead of all the individual addresses it represents. You can assign up to eight ranges in an OSPF area. In Figure 30 (page 200), routers R2 and R5 are ABRs because they both have membership in more than one area.

**Figure 30 Example of deploying ABRs to connect areas to the backbone**

Autonomous system boundary router (ASBR)

This type of OSPF router runs multiple interior gateway protocols and serves as a gateway to other autonomous systems operating with interior gateway protocols. The ASBR imports and translates different protocol routes into OSPF through redistribution. ASBRs can be used in backbone areas, normal areas, and NSSAs, but not in stub areas. For more details on redistribution and configuration examples, see “Enabling route redistribution” (page 161).

Designated routers (DRs)

In an OSPF network having two or more routers, one router is elected to serve as the DR and another router to act as the BDR. All other routers in the area forward their routing information to the DR and BDR, and the DR forwards this information to all of the routers in the network. This minimizes the amount of repetitive information that is forwarded on the network by eliminating the need for each individual router in the area to forward its routing information to all other routers in the network. If the area includes multiple networks, each network elects its own DR and BDR.

In an OSPF network with no DR and no BDR, the neighboring router with the highest priority is elected the DR, and the router with the next highest priority is elected the BDR. If the DR goes off-line, the BDR automatically becomes the DR, and the router with the next highest priority then becomes the new BDR. If multiple HP routing switches on the same OSPF network are declaring themselves DRs, both priority and router ID are used to select the DR and BDRs.

Priority is configurable by using the `vlan vid ip ospf priority 0-255` command at the interface level. You can use this parameter to help bias one router as the DR. For more on this command, see “Changing priority per-interface” (page 168). If two neighbors share the same priority, the router with the highest router ID is designated the DR. The router with the next highest router ID is designated the BDR.
For example, in Figure 31 (page 201), the DR and BDR for 10.10.10.0 network in area 5 are determined as follows:

<table>
<thead>
<tr>
<th>Router</th>
<th>Priority</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router A</td>
<td>0</td>
<td>Cannot become a DR or BDR</td>
</tr>
<tr>
<td>Router B</td>
<td>1</td>
<td>DR for the 10.10.10.0 network</td>
</tr>
<tr>
<td>Router C</td>
<td>2</td>
<td>BDR for the 10.10.10.0 network</td>
</tr>
<tr>
<td>Router D</td>
<td>3</td>
<td>Cannot become a DR or BDR</td>
</tr>
<tr>
<td>Router E</td>
<td>4</td>
<td>Becomes the new BDR if router B becomes unavailable and router C becomes the new DR</td>
</tr>
</tbody>
</table>

Figure 31 Example of DRs in an OSPF area

To learn the router priority on an interface, use the `show ip ospf interface` command and check the Pri setting under OSPF interface configuration.

**NOTE:** By default, the router ID is typically the lowest-numbered IP address or the lowest-numbered (user-configured) loopback interface configured on the device. For more information or to change the router ID, see “Changing the router ID” (page 126).

If multiple networks exist in the same OSPF area, the recommended approach is to ensure that each network uses a different router as its DR. Otherwise, if a router is a DR for more than one network, latency in the router could increase because of the increased traffic load resulting from multiple DR assignments.

When only one router on an OSPF 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:

- Interface is in a waiting state and the wait time expires
- Interface is in a waiting state and a hello packet is received that addresses the BDR
- Change in the neighbor state occurs, such as:
  - Neighbor state transitions from 2 or higher
  - Communication to a neighbor is lost
  - Neighbor declares itself to be the DR or BDR for the first time

**OSPF area types**

OSPF is built upon a hierarchy of network areas. All areas for a given OSPF domain reside in the same AS. An AS is defined as a number of contiguous networks, all of which share the same interior gateway routing protocol.

An AS can be divided into multiple areas. Each area represents a collection of contiguous networks and hosts, and the topology of a given area is not known by the internal routers in any other area. Areas define the boundaries to which types 1 and 2 LSAs are broadcast, which limits the amount of LSA flooding that occurs within the AS and also helps to control the size of the LSDBs maintained in OSPF routers. An area is represented in OSPF by either an IP address or a number. Area types include:

<table>
<thead>
<tr>
<th>Backbone</th>
<th>Not-so-stubby (NSSA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Stub</td>
</tr>
</tbody>
</table>

All areas in an AS must connect with the backbone through one or more ABRs. If a normal area is not directly connected to the backbone area, it must be configured with a virtual link to an ABR that is directly connected to the backbone. The remaining area types do not allow virtual link connections to the backbone area.

**Figure 32 Example of an AS with multiple areas and external routes**

**Backbone area**

Every AS must have one (and only one) backbone area (identified as area 0 or 0.0.0.0). The ABRs of all other areas in the same AS connect to the backbone area, either physically through an ABR or through a configured, virtual link. The backbone is a transit area that carries the type-3 summary LSAs, type-5 AS external link LSAs and routed traffic between non-backbone areas, as well as the
type-1 and type-2 LSAs and routed traffic internal to the area. ASBRs are allowed in backbone areas.

**Normal area**

This area connects to the AS backbone area through one or more ABRs (physically or through a virtual link) and supports type-3 summary LSAs and type-5 external link LSAs to and from the backbone area. ASBRs are allowed in normal areas.

**Not-so-stubby-area (NSSA)**

Beginning with software release K.12.xx, this area is available and connects to the backbone area through one or more ABRs. NSSAs are intended for use where an ASBR exists in an area where you want to control the following:

- Advertising the ASBR’s external route paths to the backbone area
- Advertising the NSSA’s summary routes to the backbone area
- Allowing LSAs from the backbone area to advertise in the NSSA:
  - Summary routes (type-3 LSAs) from other areas
  - External routes (type-5 LSAs) from other areas as a default external route (type-7 LSAs)

In the above operation, the ASBR in the NSSA injects external routes as type 7 LSAs. (Type 5 LSAs are not allowed in an NSSA.) The ABR connecting the NSSA to the backbone converts the type 7 LSAs to type 5 LSAs and injects them into the backbone area for propagation to networks in the backbone and to any normal areas configured in the AS. The ABR also injects type-3 summary LSAs:

- From the NSSA into the backbone area
- From the backbone into the NSSA

If the ABR detects type-5 external LSAs on the backbone, it injects a corresponding type-7 LSA default route (0.0.0.0/0) into the NSSA.

You can also configure the NSSA ABR to do the following:

- Suppress advertising some or all of the area’s summarized internal or external routes into the backbone area. See “Configuring ranges on an ABR to reduce advertising to the backbone (optional)” (page 162).
- Replace all type-3 summary routes and the type-7 default route with the type-3 default summary route (0.0.0.0/0).

Virtual links are not allowed for NSSAs.

**Stub area**

This area connects to the AS backbone through one or more ABRs. It does not allow an internal ASBR, and does not allow external (type 5) LSAs. A stub area supports these actions:

- Advertise the area’s summary routes to the backbone area.
- Advertise summary routes from other areas.
- Use the default summary (type-3) route to advertise both of the following:
  - Summary routes to other areas in the AS
  - External routes to other ASs
You can configure the stub area ABR to do the following:

- Suppress advertising some or all of the area’s summarized internal routes into the backbone area.
- Suppress LSA traffic from other areas in the AS by replacing type-3 summary LSAs and the default external route from the backbone area with the default summary route (0.0.0.0/0).

Virtual links are not allowed for stub areas.

**OSPF RFC compliance**

The OSPF features covered in this guide comply with the following:

- RFC 2328 OSPF version 2
- RFC 3101 OSPF NSSA option (s/w release K.12.xx and greater)
- RFC 1583 (Enabled in the default OSPF configuration. See the following Note.)

**NOTE:** If all of the routers in your OSPF domain support RFC 2178, RFC 2328, or later, you should disable RFC 1583 compatibility on all routers in the domain. See “Changing the RFC 1583 OSPF compliance setting” (page 153).

**Reducing AS external LSAs and Type-3 summary LSAs**

An OSPF ASBR uses AS external LSAs to originate advertisements of a route to another routing domain, such as an RIP domain. These advertisements are

- Flooded in the area in which the ASBR operates
- Injected into the backbone area and then propagated to any other OSPF areas (except stub areas) within the local OSPF AS. If the AS includes an NSSA, there are two additional options:
  - If the NSSA includes an ASBR, you can suppress advertising some or all of its summarized external routes into the backbone area.
  - Replace all type-3 summary LSAs and the default external route from the backbone area with the default summary route (0.0.0.0/0).

In some cases, multiple ASBRs in an AS can originate equivalent external LSAs. The LSAs are equivalent when they have the same cost, the same next hop, and the same destination. In such cases, the HP switch optimizes OSPF by eliminating duplicate AS external LSAs. That is, 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 switches that flush the duplicate AS external LSAs have more memory for other OSPF data.

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.
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 of these cases, the HP switch with the higher router ID floods the AS external LSAs and the other HP 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.

Replacing type-3 summary LSAs and type-7 default external LSAs with a type-3 default route LSA

By default, a routing switch operating as an ABR for a stub area or NSSA injects non-default, summary routes (LSA type 3) into the stub areas and NSSAs. For NSSAs, the routing switch also injects a type-7 default external route. You can further reduce LSA traffic into these areas by using no-summary. This command option configures the routing switch to:

- Replace type-3 summary LSA injection into a stub area or NSSA with a type-3 default summary route (0.0.0.0/0).
- Disable injection of the type-7 default external route into an NSSA.

You can enable this behavior when you first configure the stub area or NSSA, or at a later time. For the full command to use, see “Configuring a stub or NSSA area” (page 155).

The no-summary command does not affect intra-area advertisements, meaning the switch still accepts summary LSAs from OSPF neighbors within its area and floods them to other neighbors. The switch can form adjacencies with other routers regardless of whether summarization is enabled or disabled for areas on each switch.

When you use no-summary, the change takes effect immediately. If you apply the option to a previously configured area, the switch flushes all of the summary LSAs it has generated (as an ABR) from the area.

**NOTE:** This feature applies only when the switch is configured as an ABR for a stub area or NSSA. To completely prevent summary LSAs from injection into the area, use no-summary to disable the summary LSAs on each OSPF router that is an ABR for the area.

To implement the above operation for a stub area or NSSA, enter a command such as the following:

```plaintext
HP Switch(ospf)# area 40 stub 3 no-summary
```

Equal cost multi-path routing (ECMP)

The ECMP feature allows OSPF to add routes with multiple next-hop addresses and with equal costs to a given destination in the forwarding information base (FIB) on the routing switch. For example, if you display the IP route table by entering the show ip route command, multiple next-hop routers are listed for the same destination network (210.0.9.0/24) as shown in Example 118 (page 206).
Example 18 Example of show ip route command output with multiple next-hop routes

HP Switch show ip route

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.0/8</td>
<td>10.0.8.1</td>
<td>1</td>
<td>static</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.0.8.0/21</td>
<td>DEFAULT_VLAN</td>
<td>1</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>12.0.9.0/24</td>
<td>VLAN3</td>
<td>3</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>15.0.0.0/8</td>
<td>10.0.8.1</td>
<td>1</td>
<td>static</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>21.0.9.0/24</td>
<td>162.130.101.2</td>
<td>2</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
</tr>
<tr>
<td>21.0.9.0/24</td>
<td>162.130.101.3</td>
<td>2</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
</tr>
<tr>
<td>21.0.9.0/24</td>
<td>162.130.101.4</td>
<td>2</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td></td>
<td>static</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td></td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>162.130.101.0/24</td>
<td>VLAN2</td>
<td>2</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

For a given destination network in an OSPF domain, multiple ECMP next-hop routes can be one of the following types.

- Intra-area (routes to the destination in the same OSPF area)
- Inter-area (routes to the destination through another OSPF area)
- External (routes to the destination through another AS)

Multiple ECMP next-hop routes cannot be a mixture of intra-area, inter-area, and external routes. For example, in Example 18 (page 206), the multiple next-hop routes to network 21.0.9.0/24 are all intra-area.

Also, according to the distributed algorithm used in the selection of ECMP next-hop routes:

- Intra-area routes are preferred to inter-area routes.
- Inter-area routes are preferred to external routes through a neighboring AS.

In addition, ECMP ensures that all traffic forwarded to a given host address follows the same path, which is selected from the possible next-hop routes.

For example, in Figure 33 (page 207), the ECMP inter-area routes to destination network 10.10.10.0/24 consist of the following next-hop gateway addresses: 12.0.9.2, 13.0.9.3, and 14.0.9.4.
However, the forwarding software distributes traffic across the three possible next-hop routes in such a way that all traffic for a specific host is sent to the same next-hop router.

As shown in Figure 34 (page 207), one possible distribution of traffic to host devices is:

- Traffic to host 10.10.0.1 passes through next-hop router 12.0.9.2.
- Traffic to host 10.10.0.2 passes through next-hop router 13.0.9.3.
- Traffic to host 10.10.0.3 passes through next-hop router 12.0.9.2.
- Traffic to host 10.10.0.4 passes through next-hop router 14.0.9.4.

**Table 1. Example of traffic distribution on ECMP next-hop routers**

<table>
<thead>
<tr>
<th>IP packet destination</th>
<th>Next hop used</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.1</td>
<td>12.0.9.2</td>
</tr>
<tr>
<td>10.10.0.2</td>
<td>13.0.9.3</td>
</tr>
<tr>
<td>10.10.0.3</td>
<td>12.0.9.2</td>
</tr>
<tr>
<td>10.10.0.4</td>
<td>14.0.9.4</td>
</tr>
</tbody>
</table>

**Dynamic OSPF activation and configuration**

OSPF automatically activates when enabled with `router ospf`. All configuration commands affecting OSPF (except reconfiguring the router ID) are dynamically implemented and can be used without restarting OSPF routing. (To reconfigure the router ID, see “Changing the router ID” (page 126)).
NOTE: OSPF is automatically enabled without a system reset.

General configuration steps for OSPF

To begin using OSPF on the routing switch:

1. In the global config context, use `ip routing` to enable routing (page “Enabling IP routing” (page 152)).
2. Execute `router ospf` to place the routing switch in the `ospf` context and to enable OSPF routing (page A-21).
3. Change the OSPF RFC 1583 compliance, if needed. (See “Changing the RFC 1583 OSPF compliance setting” (page 153).)
4. Use `area` to assign the areas to which the routing switch will be attached (page A-25).
5. Assign interfaces to the configured areas per-VLAN or per-subnet by moving to each VLAN context and using one of the following commands:
   - `ip ospf area ospf-area-id` assigns all interfaces in the VLAN to the same area. Use this option when there is only one IP address configured on the VLAN or you want all subnets in the VLAN to belong to the same OSPF area.
   - `ip ospf ip-address area ospf-area-id` assigns an individual subnet to the specified area.
     (See page A-8.)
6. Optional: Assign loopback interfaces to OSPF areas by using the `ip ospf area` command at the loopback interface configuration level. (See “Assigning loopback addresses to an area (optional)” (page 158).)
7. Optional: On each routing switch used as an ASBR in your OSPF domain, configure redistribution to enable importing the routes you want to make available in the domain.
   a. On an ASBR in a backbone, normal, or NSSA area where you want to import external routes, configure redistribution filters to define the external routes you do not want imported.
   b. Enable redistribution.
     See “Configuring external route redistribution in an OSPF domain (optional)” (page 160).
8. Optional: Configure ranges on ABRs to reduce inter-area route advertising.
10. Optional: Change OSPF trap generation.
11. Optional: Reconfigure default parameters in the interface context, if needed. Includes `cost`, `dead-interval`, `hello-interval`, `priority`, and others.
13. Configure virtual links for any areas not directly connected to the backbone.

Configuration rules

- If the switch is to operate as an ASBR, you must enable redistribution (step 7 (page 208)). When you do that, ASBR capability is automatically enabled. For this reason, you should first configure redistribution filters on the ASBR. Otherwise, all possible external routes will be allowed to flood the domain. (See “Configuring external route redistribution in an OSPF domain (optional)” (page 160).)
- Each VLAN interface on which you want OSPF to run must be assigned to one of the defined areas. When a VLAN interface is assigned to an area, the IP address is automatically included in the assignment. To include additional addresses, you must enable OSPF on them separately, or use the “all” option in the assignment.
OSPF global and interface settings

When first enabling OSPF, you may want to consider configuring ranges and restricting redistribution (if an ASBR is used) to avoid unwanted advertisements of external routes. You may also want to enable the OSPF trap and authentication features to enhance troubleshooting and security. However, HP generally recommends that the remaining parameters with non-null default settings be left as-is until you have the opportunity to assess OSPF operation and determine whether any adjustments to non-default settings is warranted.

**NOTE:** Set global level parameters in the `ospf` context of the CLI. To access this context level, ensure that routing is enabled, then execute `router ospf` at the global CONFIG level. For example:

```
HP Switch (config)# router ospf
HP Switch (ospf)#
```

Use the VLAN interface context to set interface level OSPF parameters for the desired VLAN. To access this context level, use `vlan vid` either to move to the VLAN context level or to specify that context from the global config level. For example, both of the following command sets achieve the same result:

```
HP Switch(config)# vlan 20
HP Switch(vlan-20)# cost 15
```

```
HP Switch(config)# vlan 20 cost 15
```

### Changing the RFC 1583 OSPF compliance setting

In OSPF domains supporting multiple external routes from different areas to the same external destination, multiple AS-external-LSAs advertising the same destination are likely to occur. This can cause routing loops and the network problems that loops typically generate. On the routing switches, if RFC 1583 compatibility is disabled, the preference rules affecting external routes are those stated in RFC-2328, which minimize the possibility of routing loops when AS-external-LSAs for the same destination originate from ASBRs in different areas. However, because all routers in an OSPF domain must support the same routing-loop prevention measures, if the domain includes any routers that support only RFC 1583 preference rules, all routers in the domain must be configured to support RFC 1583.

**NOTE:** The routing switch is configured, by default, to be compliant with the RFC 1583 OSPF V2 specification. (Use `show ip ospf general` to view the current RFC 1583 configuration setting.)

All routes in an AS should be configured with the same compliance setting for preference rules affecting external routes. Thus, if any routers in an OSPF domain support only RFC 1583, all routers must be configured with 1583 compatibility. In the default OSPF configuration, RFC 1583 support is enabled for the routing switches.

If all routers in the domain support RFC 2178 or RFC 2328, you should disable RFC 1583 compatibility on all of the routers, because conformance to these later RFCs provides more robust protection against routing loops on external routes.

### Assigning the routing switch to OSPF areas

After you globally enable OSPF on the routing switch (see “Changing the RFC 1583 OSPF compliance setting” (page 209)), use this command to assign one or more OSPF areas within your AS. A routing switch can belong to one area or to multiple areas. (Participation in a given, assigned...
area requires configuring one or more VLANs or subnets and assigning each to the desired area. See page A-8.)

- If you want the VLANs and any subnets configured on the routing switch to all reside in the same area, you need to configure only that one area. (In this case, the routing switch would operate as an internal router for the area.)
- If you want to put different VLANs or subnets on the routing switch into different areas, you need to re-execute this command for each area. (In this case, the routing switch will operate as an ABR for each of the configured areas.)

**NOTE:** Each ABR must either be directly connected to the backbone area (0) or be configured with avirtual link to the backbone area through another ABR that is directly connected to the backbone area. For information on this, see “Configuring an ABR to use a virtual link to the backbone” (page 211).

### Configuring for external route redistribution in an OSPF domain

Configuring route redistribution for OSPF establishes the routing switch as an ASBR (residing in a backbone, normal, or NSSA) for importing and translating different protocol routes from other IGP domains into an OSPF domain. The switches support redistribution for static routes, RIP routes, and directly connected routes from RIP domains into OSPF domains. When you configure redistribution for OSPF, you can specify that static, connected, or RIP routes external to the OSPF domain are imported as OSPF routes. (Likewise, RIP redistribution supports the import of static, connected, and OSPF routes into RIP routes.) The steps for configuring external route redistribution to support ASBR operation include the following:

1. Configure redistribution filters to exclude external routes that you do not want redistributed in your OSPF domain.
2. Enable route redistribution.
3. Modify the default metric for redistribution (optional).
4. Modify the redistribution metric type (optional).
5. Change the administrative distance setting (optional).

**NOTE:** Do not enable redistribution until you have used restrict to configure the redistribution filters. Otherwise, your network might become overloaded with routes that you did not intend to redistribute.

### Configuring ranges on an ABR to reduce advertising to the backbone (optional)

Configuring ranges does the following to reduce inter-area advertising:

- **Summarizing routes**
  
  Enable a routing switch operating as an ABR to use a specific IP address and mask to summarize a range of IP addresses into a single route advertisement for injection into the backbone. This results in only one address being advertised to the network instead of all the addresses within that range. This reduces LSA traffic and the resources needed to maintain routing tables.

- **Blocking routes**
  
  Prevent an ABR from advertising specific networks or subnets to the backbone area.
  Each OSPF area supports up to 8 range configurations.

### Influencing route choices by changing the administrative distance default (optional)

The administrative distance value can be left in its default configuration setting unless a change is needed to improve OSPF performance for a specific network configuration.
The switch 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 switches, the administrative distance for OSPF routes is set at 110 for all route types (external, inter-area, and intra-area).

The switch selects one route over another based on the source of the route information. To do so, the switch can use the administrative distances assigned to the sources to influence route choices. You can change the distance settings in the OSPF global context to enable preference of one route type over another.

Adjusting performance by changing the VLAN or subnet interface settings (optional)

A setting described in this section can be configured with the same value across all subnets in a VLAN or be configured on a per-interface basis with different values.

**NOTE:** Most of the OSPF interface parameters also apply to virtual link configurations. However, when used on a virtual link configuration, the OSPF context requirement is different and the parameters are applied only to the interfaces included in the virtual link. See “Changing the dead interval on a virtual link” (page 172).

Configuring OSPF interface authentication (optional)

OSPF supports two methods of authentication for each VLAN or subnet—simple password and MD5. In addition, the value can be disabled, meaning no authentication is performed. Only one method of authentication can be active on a VLAN or subnet at a time, and if one method is configured on an interface, configuring the alternative method on the same interface automatically overwrites the first method used.

In the default configuration, OSPF authentication is disabled. All interfaces in the same network or subnet must have the same authentication method (password or MD5 key chain) and credentials.

Configuring an ABR to use a virtual link to the backbone

All ABRs must have either a direct, physical or indirect, virtual 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 use a virtual link to provide a logical connection to another ABR having a direct physical connection to the area backbone. Both ABRs must belong to the same area, and this area becomes a transit area for traffic to and from the indirectly connected ABR.

**NOTE:** A backbone area can be purely virtual with no physical backbone links. Also, virtual links can be "daisy chained." If so, the virtual link may not have one end physically connected to the backbone.

Because both ABRs in a virtual link connection are in the same OSPF area, they use the same transit area ID. This setting is automatically determined by the ABRs and should match the area ID value configured on both ABRs in the virtual link.

The ABRs in a virtual link connection also identify each other with a neighbor router setting:

- On the ABR having the direct connection to the backbone area, the neighbor router is the IP address of the router interface needing a logical connection to the backbone.
- On the opposite ABR (the one needing a logical connection to the backbone), the neighbor router is the IP address of the ABR that is directly connected to the backbone.
NOTE: By default, the router ID is the lowest numbered IP address or (user-configured) loopback interface configured on the device. For more information or to change the router ID, see "Changing the Router ID" on page E-16.

When you establish an area virtual link, you must configure it on both of the ABRs (both ends of the virtual link).

Adjusting virtual link performance by changing the interface settings (optional)

The OSPF interface parameters for this process are automatically set to their default values for virtual links. No change to the defaults is usually required unless needed for specific network conditions. These parameters are a subset of the parameters described under “Adjusting performance by changing the VLAN or subnet interface settings (optional)” (page 166). (The cost and priority settings are not configurable for a virtual link, and the commands for reconfiguring the settings are accessed in the router OSPF context instead of the VLAN context.)

NOTE: The parameter settings for virtual links must be the same on the ABRs at both ends of a given link.

Configuring OSPF authentication on a virtual link

OSPF supports the same two methods of authentication for virtual links as it does for VLANs and subnets in an area—password and MD5. In the default configuration, OSPF authentication is disabled. Only one method of authentication can be active on a virtual link at a time, and if one method is configured on a virtual link, configuring the alternative method on the same link automatically replaces the first method with the second. Both ends of a virtual link must use the same authentication method (none, password, or MD5 key chain) and related credentials.(Any interfaces that share a VLAN or subnet with the interface used on an ABR for a virtual link, including intermediate routing switches, must be configured with the same OSPF authentication.)

About OSPF passive

OSPF sends LSAs to all other routers in the same AS. To limit the flooding of LSAs throughout the AS, you can configure OSPF to be passive. OSPF does not run in the AS, but it does advertise the interface as a stub link into OSPF. Routing updates are accepted by a passive interface, but not sent out.

There is a limit of 512 total active and passive interfaces, but only a total of 128 can be active interfaces.

About configuring shortest path first (SPF) scheduling

SPF scheduling (throttling) can be configured in intervals of seconds to potentially delay SPF calculations when the network is unstable or there is a change in topology. It provides a granularity of one to four seconds between SPF calculations as opposed to the current default of five seconds.

The interval for the SPF calculations is dynamically chosen, based on the frequency of topology changes in the network. The chosen interval is within user-specified ranges of values. When the network topology is unstable, SPF throttling calculates SPF scheduling intervals that are longer, until the topology is again stable.

NOTE: It is guaranteed that no SPF will be calculated within the SPF currently in effect, however, it is not guaranteed that the SPF will be calculated at the exact expiration of the timer if there have been updates. The timer may be delayed due to system constraints.
Graceful shutdown of OSPF routing

OSPF routing can be gracefully shut down on HP switches without losing packets that are in transit. OSPF neighbors are informed that the router should not be used for forwarding traffic, which allows for maintenance on the switch without interrupting traffic in the network. There is no effect on the saved switch configuration.

Prior to a switch shutdown, the CLI/SNMP `reload` command or the CLI `boot` command is executed to initiate the sending of OSPF "empty hello list" messages on the interfaces that are part of the OSPF routing configuration. After a small delay (approximately 2 seconds) that allows the messages to be transmitted on all applicable interfaces, the `boot` or `reload` command continues.

Modules operating in nonstop mode

When a switch is in standalone mode and OSPF routing is enabled, the "empty hello list" is transmitted whenever the `boot` or `reload` commands are executed.

When the switch is operating in nonstop switching mode (redundant) and a single module is being reloaded or booted, the standby module will notify neighboring switches of the management module failover. If the failover fails, the "empty hello list" is transmitted before the switch is rebooted.

When a switch is operating with multiple management modules in warm standby mode, the "empty hello list" is sent when a `reload` or `boot` command is executed. The standby management module sends out OSPF hello packets after becoming the active management module.

OSPF equal-cost multipath (ECMP) for different subnets available through the same next-hop routes

The switches support optional load-sharing across redundant links where the network offers two, three, or four equal-cost next-hop routes for traffic to different subnets. (All traffic for different hosts in the same subnet goes through the same next-hop router.)

For example, in the OSPF network shown in Figure 35 (page 213), IP load-sharing is enabled on router "A". In this case, OSPF calculates three equal-cost next-hop routes for each of the subnets and then distributes per-subnet route assignments across these three routes.

**Figure 35 Example of load-sharing traffic to different subnets through equal-cost next-hop routers**

Example of a routing table for the network in Figure 35 (page 213)

<table>
<thead>
<tr>
<th>Destination subnet</th>
<th>Router &quot;A&quot; next hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.0.0/16</td>
<td>Router &quot;C&quot;</td>
</tr>
<tr>
<td>10.2.0.0/16</td>
<td>Router &quot;D&quot;</td>
</tr>
</tbody>
</table>
IP load-sharing does not affect routed traffic to different hosts on the same subnet. That is, all traffic for different hosts on the same subnet will go through the same next-hop router. For example, if subnet 10.32.0.0 includes two servers at 10.32.0.11 and 10.32.0.22, all traffic from router "A" to these servers will go through router "B".

<table>
<thead>
<tr>
<th>Destination subnet</th>
<th>Router &quot;A&quot; next hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.0.0/16</td>
<td>Router &quot;B&quot;</td>
</tr>
<tr>
<td>10.32.0.0/16</td>
<td>Router &quot;B&quot;</td>
</tr>
<tr>
<td>10.42.0.0/16</td>
<td>Router &quot;D&quot;</td>
</tr>
</tbody>
</table>
# 8 Route Policy

## Table 35 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] [ ip</td>
<td>ipv6 prefix-list name ] [seq seq-num</td>
<td>permit</td>
<td>deny prefix /prefix-length</td>
<td>ge min-length</td>
</tr>
<tr>
<td>[ ip</td>
<td>ipv6 prefix-list name ] [seq seq-num] description description-string</td>
<td>Enters a description into a prefix list.</td>
<td>-</td>
<td>(page 217)</td>
</tr>
<tr>
<td>show [ ip</td>
<td>ipv6 prefix-list ] [name list-name] [ summary</td>
<td>detail ]</td>
<td>Displays the content of prefix lists.</td>
<td>-</td>
</tr>
<tr>
<td>route-map name [ permit</td>
<td>deny ] [seq seq-num]</td>
<td>Creates a route map and enters the route map context.</td>
<td>-</td>
<td>(page 219)</td>
</tr>
<tr>
<td>no route-map name [seq seq-num]</td>
<td>Deletes a route map or a route map sequence.</td>
<td>-</td>
<td>(page 219)</td>
<td>-</td>
</tr>
<tr>
<td>show route-map [name]</td>
<td>Displays the commands in all route maps or in a specified route map.</td>
<td>-</td>
<td>(page 220)</td>
<td>-</td>
</tr>
<tr>
<td>[no] match interface vlan vid [vid]...</td>
<td>Matches a VLAN interface.</td>
<td>-</td>
<td>(page 220)</td>
<td>-</td>
</tr>
<tr>
<td>[no] match [ ip</td>
<td>ipv6 next-hop IP-addr</td>
<td>IPv6-addr ][ IP-addr</td>
<td>IPv6-addr ] ... [no] match [ ip</td>
<td>ipv6 ] next-hop prefix-list name</td>
</tr>
<tr>
<td>[no] match [ ip</td>
<td>ipv6 ] route-source prefix-list name</td>
<td>Matches the address of an advertising router.</td>
<td>-</td>
<td>(page 221)</td>
</tr>
<tr>
<td>[no] match metric value</td>
<td>Matches the specified metric value with that of the route.</td>
<td>-</td>
<td>(page 221)</td>
<td>-</td>
</tr>
<tr>
<td>[no] match route-type external [ type-1</td>
<td>type-2 ]</td>
<td>Matches an OSPF external route metric type.</td>
<td>-</td>
<td>(page 221)</td>
</tr>
<tr>
<td>[no] match source-protocol [ connected</td>
<td>static</td>
<td>rip</td>
<td>ospf</td>
<td>ospfv3 ]</td>
</tr>
<tr>
<td>[no] match tag value</td>
<td>Matches the specified tag value with that of the route.</td>
<td>-</td>
<td>(page 222)</td>
<td>-</td>
</tr>
<tr>
<td>[no] set [ ip</td>
<td>ipv6 next-hop ] [ IP-addr</td>
<td>IPv6-addr ]</td>
<td>Sets a next hop address.</td>
<td>-</td>
</tr>
<tr>
<td>[no] set metric value</td>
<td>Sets the route metric to the specified value.</td>
<td>-</td>
<td>(page 223)</td>
<td>-</td>
</tr>
<tr>
<td>[no] set metric-type external [ type-1</td>
<td>type-2 ]</td>
<td>Sets the metric type of an OSPF external route.</td>
<td>-</td>
<td>(page 223)</td>
</tr>
<tr>
<td>[no] set tag value</td>
<td>Sets the tag value of the route.</td>
<td>-</td>
<td>(page 223)</td>
<td>-</td>
</tr>
</tbody>
</table>

For general information about route policy, see “Route policy overview” (page 223).

### Using prefix lists

Prefix lists are named lists of route prefixes. They are used to match routes for inclusion in or exclusion from route policies.
Creating prefix list entries

A prefix list can include one or more rules, each defined by a sequence number, permit or deny instruction, prefix, and range of allowed prefix lengths.

Syntax:

```
[no][ ip | ipv6 prefix-list name ][seq seq-num] [ permit | deny prefix /prefix-length ] [ge min-length] [le max-length]
```

Enters a route prefix into a prefix list.

- **name**
  - Specifies a list of either IPv4 (IP) or IPv6 prefixes.
  - Specifies the name of the prefix list to which this prefix will be added. If the named list does not exist, this command creates it.
  - To add a prefix to an existing list, specify the name of that list.

- **seq seq-num**
  - Optionally specifies a sequence number for the entry. (See discussion of sequence numbering below.)

- **permit**
  - Permits the prefix when a successful match is made.

- **deny**
  - Denies the prefix when a successful match is made.

- **prefix/prefix-length**
  - Specifies an IPv4 or IPv6 network prefix and its mask length, in CIDR notation.
  - For example: 10.1.4.1/24.

- **ge min-length**
  - Specifies a minimum mask length of the prefix to match. min-length must have a value between 1 and 32 for IPv4, or a value between 1 and 128 for IPv6.
  - This value must be greater than or equal to prefix-length. If this optional parameter is not specified, its value defaults to prefix-length.

- **le max-length**
  - Specifies a maximum mask length of the prefix to match. max-length must have a value between 1 and 32 for IPv4, or a value between 1 and 128 for IPv6.
  - This value must be greater than or equal to min-length. If this optional parameter is not specified, its value defaults to prefix-length. (If you have specified a value for min-length that is greater than prefix-length, you must explicitly specify le with a max-length value that is greater than or equal to min-length.)

```
no [ ip | ipv6 prefix-list name ]
```

Deletes the entire prefix list identified by name.

```
no [ ip | ipv6 prefix-list name ] [seq seq-num]
```

Deletes the entry with the specified sequence number from the prefix list identified by name.

Individual prefix list entries are made using separate commands in the general configuration context. All entries that have the same prefix list name are part of the
same prefix list. Thus, the following commands, taken from a **show running-config** listing, constitute two prefix lists.

```
  ip prefix-list "Odd" seq 5 permit 10.1.1.1 255.255.255.0 ge 24 le 24
  ip prefix-list "Odd" seq 10 deny 10.1.2.1 255.255.255.0 ge 24 le 24
  ip prefix-list "Odd" seq 15 permit 10.1.3.1 255.255.255.0 ge 24 le 24
  ip prefix-list "Odd" seq 20 deny 10.1.4.1 255.255.255.0 ge 24 le 24
  ip prefix-list "Even" seq 5 deny 10.1.1.1 255.255.255.0 ge 24 le 24
  ip prefix-list "Even" seq 10 permit 10.1.2.1 255.255.255.0 ge 24 le 24
  ip prefix-list "Even" seq 15 deny 10.1.3.1 255.255.255.0 ge 24 le 24
  ip prefix-list "Even" seq 20 permit 10.1.4.1 255.255.255.0 ge 24 le 24
```

Sequence numbers, which are optional, determine the order in which prefix list entries are evaluated during match operations. If you do not specify a sequence number for an entry, the switch uses a number that is 5 more than the highest sequence number already used in the list. (For the first entry in a prefix list, the default value of the sequence number is 5.) You can insert a new entry in a prefix list between two entries already in the list by specifying a sequence number for the new entry that is between the sequence numbers of the two existing entries.

**Entering a prefix list description**

Use the following command to enter a description string into an existing prefix list:

**Syntax:**

```
[ ip | ipv6 prefix-list name ][seq seq-num description description-string]
```

Enters a description into a prefix list.

- **[ ip | ipv6 ]**
  - Specifies an IPv4 (IP) or IPv6 prefix list.
- **name**
  - Specifies the name of the prefix list to which this description will be added. The prefix list must already exist.
- **seq seq-num**
  - Optionally specifies a sequence number for the description entry. The description is attached to the prefix list entry identified by that sequence number. If the prefix list does not contain an entry with that sequence number, no description is entered.
  - If you do not specify a sequence number, the description is attached to the first entry in the prefix list at the time the description is entered.
- **description-string**
  - Specifies a description string of up to 80 characters.
If you delete the entry to which the description is attached, the description is deleted also.

**Viewing prefix lists**

The `show ip prefix-list` command displays the content of prefix lists.

**Syntax:**

```
show [ ip | ipv6 prefix-list ] [name list-name] [ summary | detail ]
```

Displays the content of prefix lists.

- `[ ip | ipv6 ]` Specifies an IPv4 (IP) or IPv6 prefix list.
- `name list-name` Specifies the name of the prefix list to display. If this parameter is omitted, all prefix lists are displayed.
- `[ summary | detail ]` If neither `summary` nor `detail` is specified, the listing displays the name of the prefix list and each entry in the list (not including descriptions).
  - If `summary` is specified, the listing displays the name of the list and a summary of the entries (but not the entries themselves).
  - If `detail` is specified, the listing displays the summary information, the description (if it exists), and the entries in the list.

**Example**

In a switch that contains two prefix lists, a standard display looks like this:

```
HP Switch# show ip prefix-list

ip prefix-list Odd: 4 entries
  seq 5 permit 10.1.1.1/24 ge 24 le 24
  seq 10 deny 10.1.2.1/24 ge 24 le 24
  seq 15 permit 10.1.3.1/24 ge 24 le 24
  seq 20 deny 10.1.4.1/24 ge 24 le 24

ip prefix-list Even: 4 entries
  seq 5 deny 10.1.1.1/24 ge 24 le 24
  seq 10 permit 10.1.2.1/24 ge 24 le 24
  seq 15 deny 10.1.3.1/24 ge 24 le 24
  seq 20 permit 10.1.4.1/24 ge 24 le 24

A summary of the prefix lists looks like this:

HP Switch# show ip prefix-list summary

ip prefix-list Odd: Count:4, Range-entries: 4, Sequences: 5 - 20
ip prefix-list Even: Count:4, Range-entries: 4, Sequences: 5 - 20

A detailed display of one of the prefix lists looks like this:

HP Switch# show ip prefix-list name Even detail

ip prefix-list Even: Count:4, Range-entries: 4, Sequences: 5 - 20
seq 5 deny 10.1.1.1/24 ge 24 le 24
Description: Permit even-numbered subnets

seq 10 permit 10.1.2.1/24 ge 24 le 24
seq 15 deny 10.1.3.1/24 ge 24 le 24
seq 20 permit 10.1.4.1/24 ge 24 le 24

Creating a route map

The route-map command creates a route map sequence. It specifies a route map name, a permit or deny instruction, and, optionally, a sequence number. All sequences that have the same route map name belong to the same route map. For more information about route maps, see “Route maps” (page 224).

Syntax:

```
route-map name [ permit | deny ] [ seq seq-num ]
```

Creates a route map and enters the route map context.

- **name**
  - Specifies the name of the route map.
- **permit**
  - Instructs the policy engine to permit the route if the match succeeds.
- **deny**
  - Instructs the policy engine to deny the route if the match succeeds.
- **seq seq-num**
  - Specifies a sequence number for the route-map. If a sequence number is not specified at the first instance of the route-map name command, the switch uses a default value of 10. (See below for more information on sequence numbering.)

Deleting all or part of a route map

Use the no form of the route-map command to delete a sequence or an entire route map.

Syntax:

```
no route-map name [ seq seq-num ]
```

Deletes a route map or a route map sequence.

- **name**
  - Specifies the name of the route map.
- **seq seq-num**
  - Optional sequence number. Specifies a sequence to delete from the named route map.

  If no sequence number is specified, the entire route map is deleted.

To delete a match or set clause from a route-map, first enter the context of that route map and then issue the no form of the clause to delete it.

Example

To delete the match metric 25 clause from sequence 20 of Map4, you would use the following commands:

```
HP Switch(config)# route-map Map4 permit seq 20
HP Switch(route-map-Map4-20)# no match metric 25
```
Viewing route maps

Syntax:

```
show route-map [name]
```

Displays the commands in all route maps or in a specified route map.

**[name]**

Optionally specifies the name of a route map to display. If no name is specified, all route maps are displayed.

All sequences of a route map are displayed. For example:

```
HP Switch(config)# show route-map Map3
Routemap information

route-map "Map3" permit seq 10
  match interface vlan 11 12 13
  match metric 25
  exit
route-map "Map3" permit seq 20
  match interface vlan 21 22 23
  match metric 25
  exit
```

Using match commands

For more information, see “Match commands” (page 225).

Matching VLANs

Syntax:

```
[no] match interface vlan vid [vid]...
```

Matches a VLAN interface.

**vid**

Specifies the ID number of the VLAN to match.

**[vid]...**

Optional additional VLAN identifiers. A single command can specify multiple VLANs. A match succeeds if any of the VLANs matches (logical OR).

The `no` form of the command deletes the match clause from the sequence.

Matching prefix lists

Syntax:

```
[no] match [ ip | ipv6 ] address prefix-list name
```

Matches a prefix list.

**[ ip | ipv6 ]**

Specifies matching with a prefix list that contains either IPv4 (IP) or IPv6 addresses, respectively.

**name**

Specifies the name of the prefix list to match.

The `no` form of the command deletes the match clause from the sequence.
Matching next-hop addresses

Syntax:

```
[no] match [ ip | ipv6 ] next-hop prefix-list name
```

Matches a next hop address.

```
[ ip | ipv6 ]
```

Specifies matching with either an IPv4 (IP) or IPv6 address, respectively.

```
[ IP-addr | IPv6-addr ]
```

Specifies the IPv4 (IP) or IPv6 address, respectively, to match with.

```
[ IP-addr | IPv6-addr ...]
```

Optional additional addresses. A single command can specify multiple IPv4 (IP) or IPv6 addresses. A match succeeds if any of the addresses matches (logical OR).

```
name
```

Specifies the name of a prefix list to match the next hop against.

The no form of the command deletes the match clause from the sequence.

Matching route sources

Syntax:

```
[no] match [ ip | ipv6 ] route-source prefix-list name
```

Matches the address of an advertising router.

```
[ ip | ipv6 ]
```

Specifies matching with a prefix list that contains either IPv4 (IP) or IPv6 addresses, respectively.

```
name
```

Specifies the name of a prefix list to match the advertising router against.

The no form of the command deletes the match clause from the sequence.

Matching route metrics

Syntax:

```
[no] match metric value
```

Matches the specified metric value with that of the route.

```
value
```

Value of the route metric to match against. This is an integer value between 0 and the maximum number supported by the routing switch.

The no form of the command deletes the match clause from the sequence.

Matching metric types

Syntax:

```
[no] match route-type external [ type-1 | type-2 ]
```

Matches an OSPF external route metric type.
type-1
Matches against an OSPF external route with a type-1 metric.

type-2
Matches against an OSPF external route with a type-2 metric.

The no form of the command deletes the match clause from the sequence.

Matching source protocols

Syntax:

[no] match source-protocol [ connected | static | rip | ospf | ospfv3 ]

Matches the protocol type of the destination prefix.

connected
Matches directly connected routes.

static
Matches static routes.

rip
Matches RIP routes.

ospf
Matches OSPF routes.

ospfv3
Matches OSPFv3 routes.

The no form of the command deletes the match clause from the sequence.

Matching tags

Syntax:

[no] match tag value

Matches the specified tag value with that of the route.

value: Value of the route tag to match against. This is an integer value between 0 and the maximum number supported by the routing switch. The tag value is typically set by a set command on a different router.

The no form of the command deletes the match clause from the sequence.

Using set commands

The set commands described below are available for use in route maps. Multiple set commands may be used in a sequence of a route map.

Setting the next hop

Syntax:

[no] set [ ip | ipv6 next-hop ][ IP-addr | IPv6-addr ]

Sets a next hop address.

[ ip | ipv6 ]
Specifies setting either an IPv4 (IP) or IPv6 address, respectively.

[ IP-addr | IPv6-addr ]
Specifies the IPv4 (IP) or IPv6 address, respectively, to set.
The \texttt{no} form of the command deletes the set clause from the sequence.

**Setting the route metric**

\textbf{Syntax:}

```
[no] set metric value
```

Sets the route metric to the specified value.

```
value
```

Value to be set for the route metric. This is an integer value between 0 and the maximum number supported by the routing switch.

The \texttt{no} form of the command deletes the set clause from the sequence.

**Setting the metric type**

\textbf{Syntax:}

```
[no] set metric-type external \{ type-1 | type-2 \}
```

Sets the metric type of an OSPF external route.

```
type-1
```

Sets the metric type of an OSPF external route to type 1.

```
type-2
```

Sets the metric type of an OSPF external route to type 2.

The \texttt{no} form of the command deletes the set clause from the sequence.

**Setting the tag value**

\textbf{Syntax:}

```
[no] set tag value
```

Sets the tag value of the route.

```
value
```

Value of the route tag. This is an integer value between 0 and the maximum number supported by the routing switch.

The \texttt{no} form of the command deletes the set clause from the sequence.

**Route policy overview**

The route table in a routing switch contains routing paths to IP destinations. The traditional sources of the routing paths are:

- Directly connected destinations (no router hops)
- Static routes (manually configured by a network administrator)
- Routing protocols such as RIP or OSPF

Route policy provides an additional method for controlling entries in the route table. This approach applies predetermined policies to define how the routing switch accepts routes from peers, propagates routes to peers, and redistributes routes between different protocols. Route policy can often provide finer control and greater flexibility over route table entries than traditional methods.

Route policy is embodied in route maps, which are used to match destination routes according to IP addresses and other parameters. Optional set statements allow changing properties of the route depending on the match. Typical uses for route policy include filtering and redistribution of routes.
**Configuring route policy**

The steps in configuring a route policy are:

1. (Optional) Create any prefix lists you will use to select routes for your policy.
2. Create a route map.
3. Include match statements in your route map to define the selection criteria for routes.
4. (Optional) Include set statements in your route map to modify properties of your routes.
5. Apply the policy.

**Route maps**

Route maps are policy tools that are used to match destination prefixes, interfaces, or other route properties. Optionally, they may change the properties of the route, depending on the match.

The route map includes one or more sequences, each of which contains match statements and, optionally, set statements. When a route map is applied, its sequences are evaluated in order. If all the match statements in a sequence match the target route, the match succeeds and the route is permitted or denied according to the permit | deny instruction in the route-map command that defined the sequence; if the sequence contains set statements, they are applied to the target route. If any of the match statements in the sequence does not match the target route, the match fails and the next sequence in the route map is evaluated. If all the sequences fail to match the route, the route is denied.

If the named route map does not already exist, the route-map command creates the route map and enters the route map context. For example:

```
HP Switch(config)# route-map Map1 permit
HP Switch(route-map-Map1-10)#
```

At this point, you are ready to enter match and set commands, described below. When you have finished entering match and set commands, an exit command exits the route map context and returns to the general configuration context.
When entering match commands, most allow only one command of a given type in a sequence. (For instance, you can enter match source-protocol rip or match source-protocol ospf, but not both.) The exceptions are matching VLAN interfaces and next hops. Multiple match interface vlan vid commands are concatenated to a single command, and a match succeeds if any of the VLANs matches. For example, the following two route maps are equivalent:

```
HP Switch(config)# route-map Map2 permit
HP Switch(route-map-Map2-10)# match interface vlan 11
HP Switch(route-map-Map2-10)# match interface vlan 12
HP Switch(route-map-Map2-10)# match interface vlan 13
HP Switch(route-map-Map2-10)# ex

HP Switch(config)# route-map Map3 permit
HP Switch(route-map-Map3-10)# match interface vlan 11 12 13
HP Switch(route-map-Map3-10)# ex
```

Similarly, multiple instances of the match ip next-hop IP-addr and match ipv6 next-hop IPv6-addr commands are concatenated internally into single commands, respectively.

The general limitation of only one match command of a given type applies within a sequence. The same type of match command can be repeated in other sequences in the same route map. All of the match clauses of the sequence must match for a match to succeed. (For this purpose, multiple match interface vlan, match ip next-hop, and match ipv6 next-hop clauses are treated as a single clause. In such a clause, the interfaces or next hops are treated in logical OR fashion: if there is a match with any one of them, the match clause succeeds.)

A match sequence that contains no match commands will permit all routes. (Such a sequence may be used in a route map that denies certain routes but permits all others.)

Like most match commands, set commands allow only one command of a given type in a sequence. So, for instance, if a match sequence is successful, you can set a metric of 23, but not metrics of 23 and 25 simultaneously.

To re-enter the context of an existing route map that has only one sequence (say, to add or delete match or set statements), the sequence number is optional: `route-map name permit | deny`. If the route-map has more than one sequence, the sequence number is required: `route-map name permit | deny seq seq-num`.

To create a new sequence in an existing route map (that is, under the same route map name), use the `route-map` command with a different sequence number. Sequence numbers are significant: they determine the order of evaluation of sequences in route maps—the sequence with the lowest number is evaluated first.

**Match commands**

The match commands described in this chapter are available for use in route maps. Multiple match commands may be used in a sequence of a route map. For most commands, only one match of a given type is permitted in a sequence. For the match interface vlan vid, match ip next-hop IP-addr, and match ipv6 next-hop IPv6-addr commands, multiple instances of those commands are permitted in a single sequence, because all instances of those commands in a sequence are concatenated internally into single commands, respectively.

**Using route policy in route redistribution**

The following examples show some basic uses of route policy based on the figure below. (All subnets have 24-bit masks.)
Baseline: Intra-domain routing using default settings

Each of the routing domains in Figure 37 (page 226) is defined with simple VLANs and a basic routing configuration:

- In the RIP domains, the RIP protocol is assigned to each VLAN that a router connects to.
- Routers in the RIP domains redistribute connected routes—this is the default setting when RIP is enabled.
- For simplicity, all VLANs in the OSPF domain are assigned to the backbone area (area 0).
- Border routers (North and South) implement both RIP and OSPF protocols.

The following listing shows the running configuration for the South router, the most complicated of the routers in this example. (Not only is the South router a border router, but it also has host computers connected directly to it in both RIP and OSPF domains.)

South(config)# show run

Running configuration:
hostname "South"
module 1 type J8702A
module 3 type J9478A
ip routing
vlan 1
    name "DEFAULT_VLAN"
    untagged A19-A24,C13-C24
    ip address dhcp-bootp
    no untagged A1-A18,C1-C12
    exit
vlan 31
    name "VLAN31"
    untagged A1-A6
    ip address 10.3.31.2 255.255.255.0
    exit
vlan 33
    name "VLAN33"
    untagged A7-A12
    ip address 10.3.33.2 255.255.255.0
    exit
vlan 21
    name "VLAN21"
    untagged A13-A18
    ip address 10.2.21.1 255.255.255.0
    exit
vlan 37
    name "VLAN37"
    untagged C1-C6
    ip address 10.3.37.1 255.255.255.0
    exit
vlan 29
    name "VLAN29"
    untagged C7-C12
    ip address 10.2.29.1 255.255.255.0
    exit
router ospf
    area backbone
    exit
router rip
    redistribute connected
    exit
snmp-server community "public" unrestricted
vlan 21
    ip rip 10.2.21.1
    exit
vlan 29
    ip rip 10.2.29.1
    exit
vlan 31
    ip ospf 10.3.31.2 area backbone
    exit
vlan 33
    ip ospf 10.3.33.2 area backbone
    exit
vlan 37
    ip ospf 10.3.37.1 area backbone
    exit
Items of particular interest are:

- The `ip routing` command enables routing on the switch.
- The `router ospf` command enables OSPF routing on the switch. The `area backbone` command establishes the backbone area (area 0).
- The `router rip` command enables RIP routing on the switch. The `redistribute connected` command redistributes directly connected routes to all routers in the attached RIP domain.
- The `vlan` commands at the end of the configuration assign routing protocols to the VLANs. Additionally, they make area assignments for VLANs in the OSPF domain.

The other routers have analogous, if somewhat simpler, routing configurations. The Northwest, Northeast, and Southeast routers have only RIP enabled, and the East router has only OSPF enabled. The North router enables both routing protocols, but has fewer VLANs.

Listed below are the routing tables that result for three representative routers:

**South**
A border router attached to both RIP and OSPF domains.

**East**
A router within the OSPF domain.

**Southeast**
A router within the RIP domain.

South(config)# show ip route

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN</th>
<th>Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.21.0/24</td>
<td>VLAN21</td>
<td>21</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.2.22.0/24</td>
<td>10.2.21.2</td>
<td>21</td>
<td>rip</td>
<td></td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.2.23.0/24</td>
<td>10.2.21.2</td>
<td>21</td>
<td>rip</td>
<td></td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.2.29.0/24</td>
<td>VLAN29</td>
<td>29</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>VLAN31</td>
<td>31</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.32.0/24</td>
<td>10.3.31.1</td>
<td>31</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.32.0/24</td>
<td>10.3.33.1</td>
<td>33</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.33.0/24</td>
<td>VLAN33</td>
<td>33</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.34.0/24</td>
<td>10.3.33.1</td>
<td>33</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.37.0/24</td>
<td>VLAN37</td>
<td>37</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td></td>
<td>static</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td></td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

East(config)# show ip route

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN</th>
<th>Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.32.0/24</td>
<td>VLAN32</td>
<td>32</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.33.0/24</td>
<td>VLAN33</td>
<td>33</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.34.0/24</td>
<td>VLAN34</td>
<td>34</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.37.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td></td>
<td>static</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td></td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Southeast(config)# show ip route

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN</th>
<th>Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.32.0/24</td>
<td>VLAN32</td>
<td>32</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.33.0/24</td>
<td>VLAN33</td>
<td>33</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.34.0/24</td>
<td>VLAN34</td>
<td>34</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.37.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td></td>
<td>static</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td></td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
With this configuration, the routers and host computers in each routing domain are able to communicate with all other routers and hosts in that domain. In addition, the routers and hosts in the RIP domains can communicate with all interfaces of the adjacent border router and with hosts attached to those interfaces. (To prevent that cross-domain communication, you would remove the `redistribute connected` command from the `router rip` context.) Beyond those connected routes on the RIP side, there is no inter-domain communication.

Thus, host Z can ping host X and host L, but not host M or host B. And host M can ping host L, but not host X or host Y or host A. And so on.

### Basic inter-domain protocol redistribution

Route redistribution allows border routers to distribute routes between adjacent routing domains. Thus, the North router can redistribute routes from the northern RIP domain to the OSPF domain and from the OSPF domain to the northern RIP domain. Similarly, the South router can redistribute routes from the southern RIP domain to the OSPF domain and from the OSPF domain to the southern RIP domain. And if both the North and South routers have redistribution enabled in both directions at the same time, the routes that are redistributed from the RIP domains to the OSPF domain will be further distributed to the opposite RIP domain, and routers and hosts in all domains will be able to communicate with each other. (Some subtle complications are explained below.)

For example, in the North and South routers you might add a `redistribute rip` command to the `router ospf` context and a `redistribute ospf` command to the `router rip` context, like this:

```
  .
  .
  router ospf
  area backbone
  redistribute rip
  exit
  router rip
  redistribute connected
  redistribute ospf
  exit
  .
  .
```

This causes extensive redistribution of routes within all three routing domains, adding a large number of routes to the route tables of all the routers. For example, the route table in the East router adds routes to subnets in both RIP domains, and looks like this:

```
East(config)# show ip route

IP Route Entries

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.1.12.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.1.14.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
</tbody>
</table>
```
10.2.22.0/24 10.3.33.2 33 ospf External2 10 110
10.2.23.0/24 10.3.33.2 33 ospf External2 10 110
10.3.31.0/24 10.3.32.1 32 ospf IntraArea 2 110
10.3.31.0/24 10.3.33.2 33 ospf IntraArea 2 110
10.3.32.0/24 VLAN32 32 connected 1 0
10.3.33.0/24 VLAN33 33 connected 1 0
10.3.34.0/24 VLAN34 34 connected 1 0
10.3.37.0/24 10.3.33.2 33 ospf IntraArea 2 110
127.0.0.0/8 reject static 0 0
127.0.0.1/32 lo0 connected 1 0

But this route table does not include all the possible routes in all domains: routes to subnets 10.1.15.x, 10.1.16.x, 10.2.21.x, and 10.2.29.x (VLANs 15, 16, 21, and 29) are missing. Host computer M cannot ping host X because there is no route to it, though it can ping through the "invisible" South router to host Y or host Z.

The problem is that those missing subnets are directly connected to the North and South border routers, and directly connected routes must be explicitly redistributed with a `redistribute connected` command even though they are RIP routes and RIP routes were redistributed. So by adding `redistribute connected` commands to the `router ospf` contexts of the North and South routers, like this:

```
  .
  .
  router ospf
  area backbone
  redistribute connected
  redistribute rip
  exit
  .
  .
```

All existing routes are redistributed and the route table for the East router is now complete:

East(config)# show ip route

```
IP Route Entries

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.12.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.14.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.15.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.16.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.21.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.22.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.23.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.29.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.32.0/24</td>
<td>VLAN32</td>
<td>32</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.33.0/24</td>
<td>VLAN33</td>
<td>33</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.34.0/24</td>
<td>VLAN34</td>
<td>34</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.37.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td>static</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td>connected</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

Host L can now ping host X and, indeed, any other host in any of the three routing domains.

**Finer control of inter-domain routing using route policy**

The wide variety of match types available with route policy allows you to make finer distinctions when distributing routes across routing domain boundaries.
Suppose that you want to limit the distribution of the "non-connected" routes in the northern RIP domain to the "odd-numbered" prefixes—that is, to 10.1.11.x and 10.1.13.x. You can accomplish that by creating a prefix list:

```
ip prefix-list "Odds" seq 5 permit 10.1.11.1 255.255.255.0 ge 24 le 24
ip prefix-list "Odds" seq 10 permit 10.1.13.1 255.255.255.0 ge 24 le 24
```

Then matching that prefix-list in a route map:

```
route-map "PermitOdds" permit seq 10
    match ip address prefix-list "Odds"
exit
```

And finally applying that route map to the redistribution of RIP routes in the North router:

```
routing ospf
    area backbone
    redistribute connected
    redistribute rip route-map "PermitOdds"
exit
```

The result of this is to permit redistribution of routes 10.1.11.x and 10.1.13.x, and to deny redistribution of routes 10.1.12.x and 10.1.14.x. (Routes 10.1.15.x and 10.1.16.x are redistributed by the redistribute connected command.) This occurs throughout the OSPF domain, and is propagated through redistribution by the South router into the southern RIP domain.

For instance, in the OSPF domain the route map of the East router becomes:

```
East(config)# show ip route
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.15.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.16.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.21.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.22.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.23.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.29.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.32.0/24</td>
<td>VLAN32</td>
<td>32</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.33.0/24</td>
<td>VLAN33</td>
<td>33</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.34.0/24</td>
<td>VLAN34</td>
<td>34</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.37.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td>static</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td>connected</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

In the southern RIP domain, the route map of the Southeast router becomes:

```
Southeast(config)# show ip route
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
</tbody>
</table>
To not lose the “even-numbered” routes (10.1.12.x and 10.1.14.x) in the OSPF domain, reinstate the original redistribution in the North router:

```
router ospf
  area backbone
  redistribute connected
  redistribute rip
  exit
```

And move the prefix list, route map, and redistribution from the North router to the South router. To get the same distribution of routes from the northern RIP to the southern RIP domain, add the 10.1.15.x and 10.1.16.x routes to the prefix list—they will not be redistributed by the redistribute connected command because they are not directly connected to the South router. The prefix list would expand to:

```
ip prefix-list "Odds" seq 5 permit 10.1.11.1 255.255.255.0 ge 24 le 24
ip prefix-list "Odds" seq 10 permit 10.1.13.1 255.255.255.0 ge 24 le 24
ip prefix-list "Odds" seq 15 permit 10.1.15.1 255.255.255.0 ge 24 le 24
ip prefix-list "Odds" seq 20 permit 10.1.16.1 255.255.255.0 ge 24 le 24
```

The route map would move from North to South with no changes:

```
route-map "Odds" permit seq 10
  match ip address prefix-list "PermitOdds"
  exit
```

And the route redistribution would move from the router ospf context to the router rip context:

```
router rip
  redistribute connected
  redistribute ospf route-map "PermitOdds"
  exit
```

This has the desired effect of redistributing all the routes in the OSPF domain, as indicated by the East router’s route table:

```
East(config)# show ip route
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.1.12.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.1.14.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.1.15.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.1.16.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.2.21.0/24</td>
<td>10.3.33.2</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
<tr>
<td>10.2.22.0/24</td>
<td>10.3.33.2</td>
<td>32</td>
<td>ospf</td>
<td>External2</td>
<td>10</td>
</tr>
</tbody>
</table>

232 Route Policy
However, it falls short in the southern RIP domain. The northern RIP routes are distributed as expected, but some of the routes from the OSPF domain are missing — 10.3.32.x and 10.3.34.x. Here is the Southeast router’s route table:

```
Southeast(config)# show ip route
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.15.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.16.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.2.21.0/24</td>
<td>VLAN21</td>
<td>21</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.2.22.0/24</td>
<td>VLAN22</td>
<td>22</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.2.23.0/24</td>
<td>VLAN23</td>
<td>23</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.2.29.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.3.33.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.3.37.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td>static</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

You can solve this problem by adding a second sequence to the route map to deal with the routes from the OSPF domain. The expanded route map becomes:

```
route-map "PermitOdds" permit seq 10
  match ip address prefix-list "Odds"
  exit
route-map "PermitOdds" permit seq 20
  match source-protocol ospf
  exit
```

Now all the desired routes show up in the Southeast router’s route table:

```
Southeast(config)# show ip route
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.15.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.16.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.2.21.0/24</td>
<td>VLAN21</td>
<td>21</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.2.22.0/24</td>
<td>VLAN22</td>
<td>22</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.2.23.0/24</td>
<td>VLAN23</td>
<td>23</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.2.29.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.3.32.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.3.33.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.3.34.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td>2</td>
<td>120</td>
</tr>
</tbody>
</table>

Using route policy in route redistribution
In addition to using route maps to filter routes, you can also use them to apply properties to the routes. For example, to apply a route metric when redistributing routes from the northern RIP domain to the OSPF domain, you could apply the metric with a `set metric` command in a route map in the North router:

```
route-map "Metric25" permit seq 10
  match source-protocol rip
  set metric 25
exit
```

Then you could redistribute from the `router ospf` context:

```
router ospf
  area backbone
  redistribute connected
  redistribute rip route-map "Metric25"
exit
```

The results are displayed in the Metric column of the East router’s route map:

```
East(config)# show ip route

IP Route Entries

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>25</td>
<td>110</td>
</tr>
<tr>
<td>10.1.12.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>25</td>
<td>110</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>25</td>
<td>110</td>
</tr>
<tr>
<td>10.1.14.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>25</td>
<td>110</td>
</tr>
<tr>
<td>10.1.15.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.1.16.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.21.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.22.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.23.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.2.29.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>10</td>
<td>110</td>
</tr>
<tr>
<td>10.3.31.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>ospf</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.32.0/24</td>
<td>10.3.32.1</td>
<td>32</td>
<td>IntraArea</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>10.3.33.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.34.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.3.37.0/24</td>
<td>10.3.33.2</td>
<td>33</td>
<td>ospf</td>
<td>2</td>
<td>110</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td></td>
<td>static</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td></td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Redistribution using tags

Tags provide an alternative method for redistributing routes. For instance, you can set tags when redistributing routes into a domain and then use those tags for matches when redistributing those routes out of the domain. In the following example, tags are set as the routes pass through the North router from the northern RIP domain to the OSPF domain, and those tags are used for matching when the routes pass out of the OSPF domain through the South router to the southern RIP domain.

Establish prefix lists on the North router to separate the "odd" and "even" routes:

```
ip prefix-list "Odds" seq 5 permit 10.1.11.0 255.255.255.0 ge 24 le 24
ip prefix-list "Odds" seq 10 permit 10.1.13.0 255.255.255.0 ge 24 le 24
```
Then set up a route map with separate sequences to tag the odd and even routes:

route-map "TagIn" permit seq 10
match ip address prefix-list "Odds"
set tag 1
exit
route-map "TagIn" permit seq 20
match ip address prefix-list "Evens"
set tag 2
exit

Set up a separate route map to match the connected routes, and assign the same tag value you used for the odd routes. This allows you to propagate both the odd and the connected routes, but not the even routes, to the southern RIP domain.

route-map "TagConn" permit seq 10
match source-protocol connected
set tag 1
exit

Redistribute the routes to the OSPF domain using the route maps:

router ospf
area backbone
  redistribute connected route-map "TagConn"
  redistribute rip route-map "TagIn"
exit

On the South router set up a route map with three sequences:

- One to permit routes with tag values of 1
- One to deny routes with tag values of 2
- One to permit OSPF routes (this propagates all the routes from the OSPF domain)

The route map looks like this:

route-map "TagOut" permit seq 10
match tag 1
exit
route-map "TagOut" deny seq 20
match tag 2
exit
route-map "TagOut" permit seq 30
match source-protocol ospf

This arrangement permits the odd routes from the northern RIP domain and the RIP routes that were connected to the North router. It denies the even routes from the northern RIP domain, and it permits the OSPF routes. The route table from the Southeast router shows the results:

Southeast(config)# show ip route

IP Route Entries

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN</th>
<th>Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.11.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td></td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.13.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td></td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.15.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td></td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.1.16.0/24</td>
<td>10.2.21.1</td>
<td>21</td>
<td>rip</td>
<td></td>
<td>2</td>
<td>120</td>
</tr>
<tr>
<td>10.2.21.0/24</td>
<td>VLAN21</td>
<td>21</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.2.22.0/24</td>
<td>VLAN22</td>
<td>22</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
| Network          | Next Hop       | metric | protocol | hop count | metric
|------------------|----------------|--------|----------|-----------|--------
| 10.2.23.0/24     | VLAN23         | 23     | connected| 1         | 0      
| 10.2.29.0/24     | 10.2.21.1      | 21     | rip      | 2         | 120    
| 10.3.31.0/24     | 10.2.21.1      | 21     | rip      | 2         | 120    
| 10.3.32.0/24     | 10.2.21.1      | 21     | rip      | 2         | 120    
| 10.3.33.0/24     | 10.2.21.1      | 21     | rip      | 2         | 120    
| 10.3.34.0/24     | 10.2.21.1      | 21     | rip      | 2         | 120    
| 10.3.37.0/24     | 10.2.21.1      | 21     | rip      | 2         | 120    
| 127.0.0.0/8      | reject         | static |          | 0         | 0      
| 127.0.0.1/32     | lo0            | connected | 1   | 0      |
9 ICMP Router Discovery Protocol

The ICMP Router Discovery Protocol (IRDP) is used by HP routing switches to advertise the IP addresses of their router interfaces to directly attached hosts. IRDP is disabled by default. You can enable the feature on a global basis or on an individual VLAN interface basis.

Configuring IRDP

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

Enter the following command:

```
HP Switch(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 Switch(config)# vlan 1
HP Switch(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
```

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**

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**

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**

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**

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.
Viewing IRDP information

To display IRDP information, enter `show ip irdp` from any CLI level.

**Example of output for `show ip irdp`**

```
HP Switch# show ip irdp

Status and Counters - ICMP Router Discovery Protocol

Global Status : Disabled

<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>
```
The Dynamic Host Configuration Protocol (DHCP) is used for configuring hosts with IP address and other configuration parameters without user intervention. The protocol is composed of three components:

- **DHCP client**
- **DHCP server**
- **DHCP relay agent**

For more information, see “Overview of DHCP” (page 249).

### Enabling DHCP relay

The DHCP relay function is enabled by default on an HP routing switch. However, if DHCP has been disabled, you can re-enable it by entering the following command at the global configuration level:

```
HP Switch(config)# dhcp-relay
```

To disable the DHCP relay function, enter the `no` form of the command:

```
HP Switch(config)# no dhcp-relay
```

### Table 36 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip bootp-gateway ip-addr</code></td>
<td>Allows you to configure an IP address for the DHCP relay agent to use for DHCP requests.</td>
<td>Lowest numbered IP address</td>
<td>(page 241)</td>
<td>-</td>
</tr>
<tr>
<td><code>show dhcp-relay bootp-gateway [vlan vid]</code></td>
<td>Displays the configured BOOTP gateway for a specified VLAN (interface).</td>
<td>-</td>
<td>(page 242)</td>
<td>-</td>
</tr>
<tr>
<td><code>ip helper-address</code></td>
<td>Adds the IP address of a DHCP server for a specified VLAN on a routing switch.</td>
<td>-</td>
<td>(page 242)</td>
<td>-</td>
</tr>
<tr>
<td><code>no dhcp-relay hop-count-increment</code></td>
<td>Disables the default behavior of a DHCP relay agent so that the hop count in a DHCP client request is not increased by one at each hop when it is forwarded to a DHCP server.</td>
<td>Hop count increases by 1 at each hop</td>
<td>(page 243)</td>
<td>-</td>
</tr>
<tr>
<td><code>show ip helper-address [vlan vlan-id]</code></td>
<td>Displays the IP helper addresses of DHCP servers configured for all static VLANs in the switch or on a specified VLAN.</td>
<td>-</td>
<td>(page 244)</td>
<td>-</td>
</tr>
<tr>
<td><code>show dhcp-relay</code></td>
<td>Displays the current setting for increasing the hop count in DHCP requests.</td>
<td>-</td>
<td>(page 244)</td>
<td>-</td>
</tr>
<tr>
<td><code>show system-information</code></td>
<td>Displays the MAC address for a given routing switch.</td>
<td>-</td>
<td>(page 245)</td>
<td>-</td>
</tr>
<tr>
<td>`dhcp-relay option 82 [ append [validate]</td>
<td>replace [validate]</td>
<td>drop [validate]</td>
<td>keep ] [ ip</td>
<td>mac</td>
</tr>
</tbody>
</table>
Using DCHP Option 12 to send a hostname

This feature allows you to include the hostname in the DHCP packet sent to the DHCP server. This is disabled by default. The command must be executed from the global configuration level.

**Syntax:**

```
[no] dhcp host-name-option
```

Sends the hostname option with DHCP packets. Use the `no` form of the command to not include the hostname in the packet.

The maximum size of the hostname is 32 characters.

Default: disabled

**Example 120 DHCP Option 12 command**

```
HP Switch(config)# dhcp host-name-option
```

**SNMP support**

A MIB object supports enabling and disabling the DHCP Option 12 feature. It is added in the `hpicfDhcpclient.mib`. The hostname is retrieved from the MIB variable `SYSNAME`. Validity checks on the name include:

- The name starts with a letter, ends with a letter or a digit, and can have letters, hyphens, or digits in between the first and last characters.
- The maximum size supported for a hostname is 30 characters. If `SYSNAME` is more than 30 characters, then DHCP Option 12 will not be included in the packet.
- The minimum number of characters supported for a hostname is one character. If the `SYSNAME` in the MIB is null, then DHCP Option 12 will not be included in the packet.

**Configuring a BOOTP/DHCP relay gateway**

The DHCP relay agent selects the lowest-numbered IP address on the interface to use for DHCP messages. The DHCP server then uses this IP address when it assigns client addresses. However, this IP address may not be the same subnet as the one on which the client needs the DHCP service. This feature provides a way to configure a gateway address for the DHCP relay agent to use for DHCP requests, rather than the DHCP relay agent automatically assigning the lowest-numbered IP address.

You must be in VLAN context to use this command, for example:

```
HP Switch# config
HP Switch(config)# vlan 1
HP Switch(vlan-1)#
```

**Syntax:**

```
ip bootp-gateway ip-addr
```

Allows you to configure an IP address for the DHCP relay agent to use for DHCP requests. The IP address must have been configured on the interface.

Default: Lowest-numbered IP address

If the IP address has not already been configured on the interface (VLAN), you will see the message shown in Example 121 (page 242).
**Example 1** Example of trying to configure an IP address that is not on this interface (VLAN)

HP Switch# config
HP Switch(config)# vlan 1
HP Switch(vlan-1)# ip bootp-gateway 10.10.10.1
The IP address 10.10.10.1 is not configured on this VLAN.

**Viewing the BOOTP gateway**

To display the configured BOOTP gateway for an interface (VLAN) or all interfaces, enter this command. You do not need to be in VLAN context mode.

**Syntax:**

```
show dhcp-relay bootp-gateway [vlan vid]
```

Displays the configured BOOTP gateway for a specified VLAN (interface). If a specific VLAN ID is not entered, all VLANs and their configured BOOTP gateways display.

**Example**

Example 122 (page 242) shows an IP address being assigned to a gateway for VLAN 22, and then displayed using the `show dhcp-relay bootp-gateway` command.

**Example 122 Assigning a gateway to an interface and then displaying the information**

HP Switch(vlan-22)# ip bootp-gateway 12.16.18.33
HP Switch(vlan-22)# exit
HP Switch(config)# show dhcp-relay bootp-gateway vlan 22

<table>
<thead>
<tr>
<th>VLAN</th>
<th>BOOTP Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN 22</td>
<td>12.16.18.33</td>
</tr>
</tbody>
</table>

**Operating notes**

- If the configured BOOTP gateway address becomes invalid, the DHCP relay agent returns to the default behavior (assigning the lowest-numbered IP address).
- If you try to configure an IP address that is not assigned to that interface, the configuration fails and the previously configured address (if there is one) or the default address is used.

**Configuring an IP helper address**

To add the IP address of a DHCP server for a specified VLAN on a routing switch, enter the `ip helper-address` command at the VLAN configuration level as in the following example:

HP Switch(config)# vlan 1
HP Switch(vlan-1)# ip helper-address ip-addr

To remove the DHCP server helper address, enter the `no` form of the command:

HP Switch(vlan-1)# no ip helper-address ip-addr
Operating notes

- You can configure up to 4000 IP helper addresses on a routing switch. The helper addresses are shared between the DHCP relay agent and UDP forwarder feature.
- A maximum of sixteen IP helper addresses is supported in each VLAN.

Disabling the hop count in DHCP requests

For more information, see “Hop count in DHCP requests” (page 249).

To disable the default behavior of a DHCP relay agent so that the hop count in a DHCP client request is not increased by one at each hop when it is forwarded to a DHCP server, enter the `no dhcp-relay hop-count-increment` command at the global configuration level:

```
HP Switch(config)# no dhcp-relay hop-count-increment
```

To reset the default function, which increases the hop count in each DHCP request forwarded to a DHCP server, enter the following command:

```
HP Switch(config)# dhcp-relay hop-count-increment
```

Operating notes

- By default, the DHCP relay agent increases the hop count in each DHCP request by one. You must enter the `no dhcp-relay hop-count-increment` command to disable this function.
- You enter the `no dhcp-relay hop-count-increment` command at the global configuration level. The command is applied to all interfaces on the routing switch that are configured to forward DHCP requests.
- This DHCP relay enhancement applies only to DHCP requests forwarded to a DHCP server. The server does not change the hop count included in the DHCP response sent to DHCP clients.
- When you disable or re-enable the DHCP hop count function, no other behavior of the relay agent is affected.
- You can configure the DHCP relay hop count function only from the CLI; you cannot configure this software feature from the drop-down menus.
- A new MIB variable, hpDhcpRelayHopCount, is introduced to support SNMP management of the hop count increment by the DHCP relay agent in a switch.

Verifying the DHCP relay configuration

Viewing the DHCP relay setting

Use the `show config` command (or `show running` for the running-config file) to display the current DHCP relay setting.

**NOTE:** The DHCP relay and hop count increment settings appear in the `show config` command output only if the non-default values are configured. For more information about the DHCP hop count increment, see “Hop count in DHCP requests” (page 249).
Example 23 Displaying startup configuration with DHCP relay and hop count increment disabled

```plaintext
HP Switch# show config
Startup configuration:
; J8697A Configuration Editor; Created on release #K.11.00
hostname "HP Switch"
cdp run
module 1 type J8702A
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
no dhcp-relay hop-count-increment
```

Non-Default DHCP Relay and Hop Count Increment settings

---

Viewing DHCP helper addresses

This command displays the list of currently configured IP Helper addresses for a specified VLAN on the switch.

**Syntax:**

```
show ip helper-address [vlan vlan-id]
```

Displays the IP helper addresses of DHCP servers configured for all static VLANs in the switch or on a specified VLAN, regardless of whether the DHCP relay feature is enabled. The `vlan vlan-id` parameter specifies a VLAN ID number.

**Example**

The following command lists the currently configured IP Helper addresses for VLAN 1.

**Example 24 Displaying IP helper addresses**

```plaintext
HP Switch(config)# show ip helper-address vlan 1

IP Helper Addresses

<table>
<thead>
<tr>
<th>IP Helper Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.28.227.97</td>
</tr>
<tr>
<td>10.29.227.53</td>
</tr>
</tbody>
</table>
```

---

Viewing the hop count setting

To verify the current setting for increasing the hop count in DHCP requests, enter the `show dhcp-relay` command. The current setting is displayed next to DHCP Request Hop Count Increment.
Example 125 Displaying hop count status

HP Switch# show dhcp-relay
Status and Counters - DHCP Relay Agent
DHCP Relay Agent Enabled : Yes
DHCP Request Hop Count Increment: Disabled
Option 82 Handle Policy : Replace
Remote ID : MAC Address

<table>
<thead>
<tr>
<th>Client Requests</th>
<th>Server Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Dropped</td>
</tr>
<tr>
<td>1425</td>
<td>2</td>
</tr>
</tbody>
</table>

Viewing the MAC address for a routing switch

To view the MAC address for a given routing switch, execute the show system-information command in the CLI.

Example 126 Using the CLI to view the switch MAC address

HP Switch(config)# show system information

Status and Counters - General System Information
System Name       : HP Switch
System Contact    :
System Location   :
MAC Age Time (sec) : 300

Time Zone : 0
Daylight Time Rule : None

Software revision : K.15.06.0000x
ROM Version       : K.15.13
Allow V1 Modules  : No

Up Time          : 32 days
CPU Util (%)     : 0
IP Mgmt - Pkts Rx : 5,372,271
Pkts Tx : 298,054

Memory - Total : 128,839,680
Free : 65,802,416
Packet - Total : 6750
Buffers Free : 5086
Lowest : 4441
Missed : 0

Configuring Option 82

For information on Option 82, see the sections beginning with “DHCP Option 82” (page 250).

Syntax:

append

Configures the switch to append an Option 82 field to the client DHCP packet. If the client packet has existing Option 82 fields assigned by another device, the new field is appended to the existing fields.

The appended Option 82 field includes the switch Circuit ID (inbound port number*) associated with the client DHCP packet and the switch Remote ID.
The default switch remote ID is the MAC address of the switch on which the packet was received from the client.

To use the incoming VLAN’s IP address or the Management VLAN IP address (if configured) for the remote ID instead of the switch MAC address, use the `ip` or `mgmt-vlan` option (below).

replace

Configures the switch to replace existing Option 82 fields in an inbound client DHCP packet with an Option 82 field for the switch.

The replacement Option 82 field includes the switch circuit ID (inbound port number*) associated with the client DHCP packet and the switch remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client.

To use the incoming VLAN’s IP address or the Management VLAN IP address (if configured) for the remote ID instead of the switch MAC address, use the `ip` or `mgmt-vlan` option (below).

drop

Configures the routing switch to unconditionally drop any client DHCP packet received with existing Option 82 fields. This means that such packets will not be forwarded. Use this option where access to the routing switch by untrusted clients is possible.

If the routing switch receives a client DHCP packet without an Option 82 field, it adds an Option 82 field to the client and forwards the packet. The added Option 82 field includes the switch circuit ID (inbound port number*) associated with the client DHCP packet and the switch remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client.

To use the incoming VLAN’s IP address or the Management VLAN IP address (if configured) for the remote ID instead of the switch MAC address, use the `ip` or `mgmt-vlan` option (below).

keep

For any client DHCP packet received with existing Option 82 fields, configures the routing switch to forward the packet as-is, without replacing or adding to the existing Option 82 fields.

validate

Operates when the routing switch is configured with append, replace, or drop as a forwarding policy. With `validate` enabled, the routing switch applies stricter rules to an incoming Option 82 server response to determine whether to forward or drop the response. For more information, see “Validation of server response packets” (page 255).

[ ip | mac | mgmt-vlan ]

Specifies the remote ID suboption that the switch uses in Option 82 fields added or appended to DHCP client packets. The type of remote ID defines DHCP policy areas in the client requests sent to the DHCP server. If a remote ID suboption is
not configured, the routing switch defaults to the **mac** option. See “Option 82 field content” (page 252).

- **ip**: Specifies the IP address of the VLAN on which the client DHCP packet enters the switch.

- **mac**: Specifies the routing switch's MAC address. (The MAC address used is the same MAC address that is assigned to all VLANs configured on the routing switch.) This is the default setting.

- **mgmt-vlan**: Specifies the IP address of the (optional) management VLAN configured on the routing switch. Requires that a management VLAN is already configured on the switch. If the management VLAN is multinetted, the primary IP address configured for the management VLAN is used for the remote ID.

If you enter the `dhcp-relay option 82` command without specifying either **ip** or **mac**, the MAC address of the switch on which the packet was received from the client is configured as the remote ID. For information about the remote ID values used in the Option 82 field appended to client requests, see “Option 82 field content” (page 252).

**Example**

In the routing switch shown below, option 82 has been configured with **mgmt-vlan** for the remote ID.

```
HP Switch(config)# dhcp-relay option 82 append mgmt-vlan
```

The resulting effect on DHCP operation for clients X, Y, and Z is shown in Table 37 (page 248).

**Figure 38 DHCP Option 82 when using the management VLAN as the remote ID suboption**

![Diagram showing DHCP Option 82 configuration](image-url)
Table 37 DHCP operation for the topology in Figure 38 (page 247)

<table>
<thead>
<tr>
<th>Client</th>
<th>Remote ID</th>
<th>giaddr1</th>
<th>DHCP server</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>10.38.10.1</td>
<td>10.39.10.1</td>
<td>A only</td>
</tr>
<tr>
<td>Y</td>
<td>10.38.10.1</td>
<td>10.29.10.1</td>
<td>B or C</td>
</tr>
<tr>
<td>Z</td>
<td>10.38.10.1</td>
<td>10.15.10.1</td>
<td>B or C</td>
</tr>
</tbody>
</table>

If a DHCP client is in the management VLAN, its DHCP requests can go only to a DHCP server that is also in the management VLAN. Routing to other VLANs is not allowed.

Clients outside of the management VLAN can send DHCP requests only to DHCP servers outside of the management VLAN. Routing to the management VLAN is not allowed.

1 The IP address of the primary DHCP relay agent receiving a client request packet is automatically added to the packet, and is identified as the giaddr (gateway interface address). This is the IP address of the VLAN on which the request packet was received from the client. For more information, see RFC 2131 and RFC 3046.

Operating notes

• This implementation of DHCP relay with Option 82 complies with the following RFCs:
  • RFC 2131
  • RFC 3046

• Moving a client to a different port allows the client to continue operating as long as the port is a member of the same VLAN as the port through which the client received its IP address. However, rebooting the client after it moves to a different port can alter the IP addressing policy the client receives if the DHCP server is configured to provide different policies to clients accessing the network through different ports.

• The IP address of the primary DHCP relay agent receiving a client request packet is automatically added to the packet, and is identified as the giaddr (gateway interface address). (That is, the giaddr is the IP address of the VLAN on which the request packet was received from the client.) For more information, see RFC 2131 and RFC 3046.

• DHCP request packets from multiple DHCP clients on the same relay agent port will be routed to the same DHCP servers. When using 802.1X on a switch, a port’s VLAN membership may be changed by a RADIUS server responding to a client authentication request. In this case the DHCP servers accessible from the port may change if the VLAN assigned by the RADIUS server has different DHCP helper addresses than the VLAN used by unauthenticated clients.

• Where multiple DHCP servers are assigned to a VLAN, a DHCP client request cannot be directed to a specific server. Thus, where a given VLAN is configured for multiple DHCP servers, all of these servers should be configured with the same IP addressing policy.

• Where routing switch "A" is configured to insert its MAC address as the remote ID in the Option 82 fields appended to DHCP client requests, and upstream DHCP servers use that MAC address as a policy boundary for assigning an IP addressing policy, then replacing switch "A" makes it necessary to reconfigure the upstream DHCP servers to recognize the MAC address of the replacement switch. This does not apply in the case where an upstream relay agent "A" is configured with option 82 replace, which removes the Option 82 field originally inserted by switch "A."

• Relay agents without Option 82 can exist in the path between Option 82 relay agents and an Option 82 server. The agents without Option 82 forward client requests and server responses without any effect on Option 82 fields in the packets.

• If the routing switch cannot add an Option 82 field to a client’s DHCP request because the message size exceeds the MTU size, the request is forwarded to the DHCP server without Option 82 data and an error message is logged in the switch’s Event Log.
Because routing is not allowed between the management VLAN and other VLANs, a DHCP server must be available in the management VLAN if clients in the management VLAN require a DHCP server.

If the management VLAN IP address configuration changes after `mgmt-vlan` has been configured as the remote ID suboption, the routing switch dynamically adjusts to the new IP addressing for all future DHCP requests.

The management VLAN and all other VLANs on the routing switch use the same MAC address.

**Overview of DHCP**

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.

HP routing switches provide the DHCP relay agent to enable communication from a DHCP server to DHCP clients on subnets other than the one the server resides on. The DHCP relay agent transfers DHCP messages from DHCP clients located on a subnet without a DHCP server to other subnets. It also relays answers from DHCP servers to DHCP clients.

The DHCP relay agent is transparent to both the client and the server. Neither side is aware of the communications that pass through the DHCP relay agent. As DHCP clients broadcast requests, the DHCP relay agent receives the packets and forwards them to the DHCP server. During this process, the DHCP relay agent increases the hop count by one before forwarding the DHCP message to the server. A DHCP server includes the hop count from the DHCP request that it receives in the response that it returns to the client.

**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 to broadcast IP address and is forwarded to all VLANs with configured IP interfaces (except the source VLAN).

**Enabling DHCP relay operation**

For the DHCP relay agent to work on the switch, you must complete the following steps:

1. Enable DHCP relay on the routing switch (the default setting).
2. Ensure that a DHCP server is servicing the routing switch.
3. Enable IP routing on the routing switch.
4. Ensure that there is a route from the DHCP server to the routing switch and back.
5. Configure one or more IP helper addresses for specified VLANs to forward DHCP requests to DHCP servers on other subnets.

**Hop count in DHCP requests**

When a DHCP client broadcasts requests, the DHCP relay agent in the routing switch receives the packets and forwards them to the DHCP server (on a different subnet, if necessary). During this
process, the DHCP relay agent increments the hop count before forwarding DHCP packets to the server. The DHCP server, in turn, includes the hop count from the received DHCP request in the response sent back to a DHCP client.

As a result, the DHCP client receives a non-zero hop count in the DHCP response packet. Because some legacy DHCP/BootP clients discard DHCP responses that contain a hop count greater than one, they may fail to boot up properly. Although this behavior is in compliance with RFC 1542, it prevents a legacy DHCP/BootP client from being automatically configured with a network IP address.

**DHCP Option 82**

Option 82 is called the relay agent information option and is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers recognizing the relay agent information option may use the information to implement IP address or other parameter assignment policies. The DHCP server echoes the option back verbatim to the relay agent in server-to-client replies, and the relay agent strips the option before forwarding the reply to the client.

The relay agent information option is organized as a single DHCP option that contains one or more suboptions that convey information known by the relay agent. The initial suboptions are defined for a relay agent that is co-located in a public circuit access unit. These include a circuit ID for the incoming circuit and a remote ID that provides a trusted identifier for the remote high-speed modem.

The routing switch can operate as a DHCP relay agent to enable communication between a client and a DHCP server on a different subnet. Without Option 82, DHCP operation modifies client IP address request packets to the extent needed to forward the packets to a DHCP server. Option 82 enhances this operation by enabling the routing switch to append an Option 82 field to such client requests. This field includes two suboptions for identifying the routing switch (by MAC address or IP address) and the routing switch port the client is using to access the network. A DHCP server with Option 82 capability can read the appended field and use this data as criteria for selecting the IP addressing it will return to the client through the usual DHCP server response packet. This operation provides several advantages over DHCP without Option 82:

- An Option 82 DHCP server can use a relay agent’s identity and client source port information to administer IP addressing policies based on client and relay agent location within the network, regardless of whether the relay agent is the client’s primary relay agent or a secondary agent.
- A routing switch operating as a primary Option 82 relay agent for DHCP clients requesting an IP address can enhance network access protection by blocking attempts to use an invalid Option 82 field to imitate an authorized client, or by blocking attempts to use response packets with missing or invalid Option 82 suboptions to imitate valid response packets from an authorized DHCP server.
- An Option 82 relay agent can also eliminate unnecessary broadcast traffic by forwarding an Option 82 DHCP server response only to the port on which the requesting client is connected, instead of broadcasting the DHCP response to all ports on the VLAN.

**NOTE:** The routing switch’s DHCP relay information (Option 82) feature can be used in networks where the DHCP servers are compliant with RFC 3046 Option 82 operation. DHCP servers that are not compliant with Option 82 operation ignore Option 82 fields. For information on configuring an Option 82 DHCP server, see the documentation provided with the server application.

Some client applications can append an Option 82 field to their DHCP requests; see the documentation provided for your client application.

It is not necessary for all relay agents on the path between a DHCP client and the server to support Option 82, and a relay agent without Option 82 should forward DHCP packets regardless of whether they include Option 82 fields. However, Option 82 relay agents should be positioned at
the DHCP policy boundaries in a network to provide maximum support and security for the IP addressing policies configured in the server.

Option 82 server support

To apply DHCP Option 82, the routing switch must operate in conjunction with a server that supports Option 82. (DHCP servers that do not support Option 82 typically ignore Option 82 fields.) Also, the routing switch applies Option 82 functionality only to client request packets being routed to a DHCP server. DHCP relay with Option 82 does not apply to switched (non-routed) client requests.

For information on configuring policies on a server running DHCP Option 82, see the documentation provided for that application.

Figure 39 Example of a DHCP Option 82 application

General DHCP Option 82 requirements and operation

Requirements

DHCP Option 82 operation is configured at the global config level and requires the following:

- IP routing enabled on the switch
- DHCP-relay option 82 enabled (global command level)
- Routing switch access to an Option 82 DHCP server on a different subnet than the clients requesting DHCP Option 82 support
- One IP helper address configured on each VLAN supporting DHCP clients

General DHCP-relay operation with Option 82

Typically, the first (primary) Option 82 relay agent to receive a client’s DHCP request packet appends an Option 82 field to the packet and forwards it toward the DHCP server identified by the IP helper address configured on the VLAN in which the client packet was received. Other, upstream relay agents used to forward the packet may append their own Option 82 fields, replace the Option 82 fields they find in the packet, forward the packet without adding another field, or drop the packet. (Intermediate next-hop routing switches without Option 82 capability can be used to forward—route—client request packets with Option 82 fields.) Response packets from an Option 82 server are routed back to the primary relay agent (routing switch) and include an IP addressing assignment for the requesting client and an exact copy of the Option 82 data the server received with the client request. The relay agent strips off the Option 82 data and forwards the response packet out the port indicated in the response as the Circuit ID (client access port). Under certain validation conditions described later in this section, a relay agent detecting invalid Option 82 data in a response packet may drop the packet.
Option 82 field content

The remote ID and circuit ID subfields comprise the Option 82 field a relay agent appends to client requests. A DHCP server configured to apply a different IP addressing policy to different areas of a network uses the values in these subfields to determine which DHCP policy to apply to a given client request.

Remote ID

This configurable subfield identifies a policy area that comprises either the routing switch as a whole (by using the routing switch MAC address) or an individual VLAN configured on the routing switch (by using the IP address of the VLAN receiving the client request).

- Use the IP address option if the server will apply different IP addressing policies to DHCP client requests from ports in different VLANs on the same routing switch.

- Use the management VLAN option if a management VLAN is configured and you want all DHCP clients on the routing switch to use the same IP address. (This is useful if you are applying the same IP addressing policy to DHCP client requests from ports in different VLANs on the same routing switch.) Configuring this option means the management VLAN’s IP address appears in the remote ID subfield of all DHCP requests originating with clients connected to the routing switch, regardless of the VLAN on which the requests originate.

- Use the MAC address option if, on a given routing switch, it does not matter to the DHCP server which VLAN is the source of a client request (that is, use the MAC address option if the IP addressing policies supported by the target DHCP server do not distinguish between client requests from ports in different VLANs in the same routing switch).

Circuit ID

This nonconfigurable subfield identifies the port number of the physical port through which the routing switch received a given DHCP client request and is necessary to identify if you want to configure an Option 82 DHCP server to use the Circuit ID to select a DHCP policy to assign to clients connected to the port. This number is the identity of the inbound port. On HP fixed-port switches, the port number used for the circuit ID is always the same as the physical port number shown on the front of the switch. On HP chassis switches, where a dedicated, sequential block of internal port numbers are reserved for each slot, regardless of whether a slot is occupied, the circuit ID for a given port is the sequential index number for that port position in the slot. (To view the index number assignments for ports in the routing switch, use the `walkmib ifname` command.)
Example 127 Using walkmib to determine the circuit ID for a port on an HP chassis

For example, the circuit ID for port B11 on an HP switch is “35”, see Example 127 (page 253), below.

```plaintext
HP Switch# walkmib ifname
ifName.1 = A1
ifName.2 = A2
ifName.3 = A3
ifName.4 = A4
ifName.25 = B1
ifName.26 = B2
ifName.27 = B3
ifName.28 = B4
ifName.29 = B5
ifName.30 = B6
ifName.31 = B7
ifName.32 = B8
ifName.33 = B9
ifName.34 = B10
ifName.35 = B11
ifName.36 = B12
ifName.37 = B13
ifName.38 = B14
ifName.39 = B15
ifName.40 = B16
ifName.41 = B17
ifName.42 = B18
ifName.43 = B19
```

The Index (and Circuit ID) number for port B11 on the routing switch.

In this example, the switch has a 4-port module installed in slot ”A” and a 24-port module installed in slot ”B”. Thus, the first port numbers in the listing are the Index numbers reserved for slot ”A”. The first Index port number for slot ”B” is ”25”, and the Index port number for port B11 (and therefore the Circuit ID number) is ”35”.

For example, suppose you want port 10 on a given relay agent to support no more than five DHCP clients simultaneously. You can configure the server to allow only five IP addressing assignments at any one time for the circuit ID (port) and remote ID (MAC address) corresponding to port 10 on the selected relay agent.

Similarly, if you want to define specific ranges of addresses for clients on different ports in the same VLAN, you can configure the server with the range of IP addresses allowed for each circuit ID (port) associated with the remote ID (IP address) for the selected VLAN.

Forwarding policies

DHCP Option 82 on HP switches offers four forwarding policies, with an optional validation of server responses for three of the policy types (append, replace, or drop).

<table>
<thead>
<tr>
<th>Option 82 configuration</th>
<th>DHCP client request packet inbound to the routing switch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Packet has no Option 82 field</td>
</tr>
<tr>
<td>Append</td>
<td>Append an Option 82 field</td>
</tr>
<tr>
<td>Option 82 configuration</td>
<td>DHCP client request packet inbound to the routing switch</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Packet has no Option 82 field</td>
</tr>
<tr>
<td><strong>NOTE:</strong> In networks with multiple relay agents between a client and an Option 82 server, append can be used only if the server supports multiple Option 82 fields in a client request. If the server supports only one Option 82 field in a request, consider using the keep option.</td>
<td></td>
</tr>
<tr>
<td>Keep</td>
<td>Append an Option 82 field</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Replace</td>
<td>Append an Option 82 field</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Drop</td>
<td>Append an Option 82 field</td>
</tr>
</tbody>
</table>

**Multiple Option 82 relay agents in a client request path**

Where the client is one router hop away from the DHCP server, only the Option 82 field from the first (and only) relay agent is used to determine the policy boundary for the server response. Where there are multiple Option 82 router hops between the client and the server, you can use different configuration options on different relay agents to achieve the results you want. This includes configuring the relay agents so that the client request arrives at the server with either one Option 82 field or multiple fields. (Using multiple Option 82 fields assumes that the server supports multiple fields and is configured to assign IP addressing policies based on the content of multiple fields.)
The above combination allows for detection and dropping of client requests with spurious Option 82 fields. If none are found, the drop policy on the first relay agent adds an Option 82 field, which is then kept unchanged over the next two relay agent hops ("B" and "C"). The server can then enforce an IP addressing policy based on the Option 82 field generated by the edge relay agent ("A"). In this example, the DHCP policy boundary is at relay agent 1.

This is an enhancement of the previous example. In this case, each hop for an accepted client request adds a new Option 82 field to the request. A DHCP server capable of using multiple Option 82 fields can be configured to use this approach to keep a more detailed control over leased IP addresses. In this example, the primary DHCP policy boundary is at relay agent "A," but more global policy boundaries can exist at relay agents "B" and "C."

Like the first example, above, this configuration drops client requests with spurious Option 82 fields from clients on the edge relay agent. However, in this case, only the Option 82 field from the last relay agent is retained for use by the DHCP server. In this case the DHCP policy boundary is at relay agent "C." In the previous two examples the boundary was with relay "A."

Validation of server response packets

A valid Option 82 server response to a client request packet includes a copy of the Option 82 fields the server received with the request. With validation disabled, most variations of Option 82 information are allowed, and the corresponding server response packets are forwarded.

Server response validation is an option you can specify when configuring Option 82 DHCP for append, replace, or drop operation. See “Forwarding policies” (page 253). Enabling validation on the routing switch can enhance protection against DHCP server responses that are either from untrusted sources or are carrying invalid Option 82 information.

With validation enabled, the relay agent applies stricter rules to variations in the Option 82 fields of incoming server responses to determine whether to forward the response to a downstream device or to drop the response due to invalid (or missing) Option 82 information. Table 38 (page 256), below, describes relay agent management of DHCP server responses with optional validation enabled and disabled.
<table>
<thead>
<tr>
<th>Response packet content</th>
<th>Option 82 configuration</th>
<th>Validation enabled on the relay agent</th>
<th>Validation disabled (the default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid DHCP server response packet without an Option 82 field.</td>
<td>append, replace, or drop¹</td>
<td>Drop the server response packet.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>keep²</td>
<td></td>
<td>Forward server response packet to a downstream device.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>The server response packet carries data indicating a given routing switch is the primary relay agent for the original client request, but the associated Option 82 field in the response contains a remote ID and circuit ID combination that did not originate with the given relay agent.</td>
<td>append</td>
<td>Drop the server response packet.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>replace or drop¹</td>
<td></td>
<td>Drop the server response packet.</td>
<td>Drop the server response packet.</td>
</tr>
<tr>
<td>keep²</td>
<td></td>
<td>Forward server response packet to a downstream device.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>The server response packet carries data indicating a given routing switch is the primary relay agent for the original client request, but the associated Option 82 field in the response contains a Remote ID that did not originate with the relay agent.</td>
<td>append</td>
<td>Drop the server response packet.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>replace or drop¹</td>
<td></td>
<td>Drop the server response packet.</td>
<td>Drop the server response packet.</td>
</tr>
<tr>
<td>keep²</td>
<td></td>
<td>Forward server response packet to a downstream device.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>All other server response packets³</td>
<td>append, keep², replace, or drop¹</td>
<td>Forward server response packet</td>
<td>Forward server response packet</td>
</tr>
</tbody>
</table>

256 Dynamic Host Configuration Protocol
Table 38 Relay agent management of DHCP server response packets. (continued)

<table>
<thead>
<tr>
<th>Response packet content</th>
<th>Option 82 configuration</th>
<th>Validation enabled on the relay agent</th>
<th>Validation disabled (the default)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>packet to a downstream device.</td>
<td>packet to a downstream device.</td>
</tr>
</tbody>
</table>

 Drop is the recommended choice because it protects against an unauthorized client inserting its own Option 82 field for an incoming request.

 A routing switch with DHCP Option 82 enabled with the keep option forwards all DHCP server response packets except those that are not valid for either Option 82 DHCP operation (compliant with RFC 3046) or DHCP operation without Option 82 support (compliant with RFC 2131).

 A routing switch with DHCP Option 82 enabled drops an inbound server response packet if the packet does not have any device identified as the primary relay agent (giaddr=null; see RFC 2131).

 Multinetted VLANs

 On a multinetted VLAN, each interface can form an Option 82 policy boundary within that VLAN if the routing switch is configured to use IP for the remote ID suboption. That is, if the routing switch is configured with IP as the remote ID option and a DHCP client request packet is received on a multinetted VLAN, the IP address used in the Option 82 field will identify the subnet on which the packet was received instead of the IP address for the VLAN. This enables an Option 82 DHCP server to support more narrowly defined DHCP policy boundaries instead of defining the boundaries at the VLAN or whole routing switch levels. If the MAC address option (the default) is configured instead, the routing switch MAC address will be used regardless of which subnet was the source of the client request. (The MAC address is the same for all VLANs configured on the routing switch.) All request packets from DHCP clients in the different subnets in the VLAN must be able to reach any DHCP server identified by the IP helper addresses configured on that VLAN.
11 User Datagram Protocol

Table 39 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] ip udp-bcast-forward</td>
<td>Enables or disables UDP broadcast forwarding on the routing switch.</td>
<td>Disabled</td>
<td>(page 258)</td>
<td>-</td>
</tr>
<tr>
<td>[no] ip forward-protocol udp ip-address [</td>
<td>Routes an inbound UDP broadcast packet received from a client on the VLAN to</td>
<td>-</td>
<td>(page 258)</td>
<td>-</td>
</tr>
<tr>
<td>port-number</td>
<td></td>
<td>the unicast or broadcast address configured for the UDP port type.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show ip forward-protocol [vlan vid]</td>
<td>Displays the current status of UDP broadcast forwarding and lists the</td>
<td>-</td>
<td>(page 259)</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>UDP forwarding addresses configured on all static VLANs in the switch or on</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>a specific VLAN.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For introductory information about user datagram protocol (UDP), see “UDP broadcast forwarding” (page 261).

Configuring and enabling UDP broadcast forwarding

To configure and enable UDP broadcast forwarding on the switch:
1. Enable routing.
2. Globally enable UDP broadcast forwarding.
3. On a per-VLAN basis, configure a forwarding address and UDP port type for each type of incoming UDP broadcast you want routed to other VLANs.

Globally enabling UDP broadcast forwarding

Syntax:

```powershell
[no] ip udp-bcast-forward
```

Enables or disables UDP broadcast forwarding on the routing switch. Routing must be enabled before executing this command.

Using the no form of this command disables any ip forward protocol udp commands configured in VLANs on the switch.

Default: Disabled

Configuring UDP broadcast forwarding on individual VLANs

This command routes an inbound UDP broadcast packet received from a client on the VLAN to the unicast or broadcast address configured for the UDP port type.

Syntax:

```powershell
[no] ip forward-protocol udp ip-address [ port-number | port-name ]
```

Used in a VLAN context to configure or remove a server or broadcast address and its associated UDP port number. You can configure a maximum of 16 forward-protocol udp assignments in a given VLAN. The switch allows a total of 256 forward-protocol udp assignments across all VLANs.
You can configure UDP broadcast forwarding addresses regardless of whether UDP broadcast forwarding is globally enabled on the switch. However, the feature does not operate unless globally enabled.

This can be either of the following:

- The unicast address of a destination server on another subnet. For example: 15.75.10.43.
- The broadcast address of the subnet on which a destination server operates. For example, the following address directs broadcasts to all hosts in the 15.75.11.0 subnet: 15.75.11.255.

**NOTE:** The subnet mask for a forwarded UDP packet is the same as the subnet mask for the VLAN (or subnet on a multinetted VLAN) on which the UDP broadcast packet was received from a client.

| **ip-address** | This can be either of the following:
|----------------|-----------------------------------------------------|
|                | • The unicast address of a destination server on another subnet. For example: 15.75.10.43.
|                | • The broadcast address of the subnet on which a destination server operates. For example, the following address directs broadcasts to all hosts in the 15.75.11.0 subnet: 15.75.11.255.
| **udp-port-#** | Any UDP port number corresponding to a UDP application supported on a device at the specified unicast address or in the subnet at the specified broadcast address. For more information on UDP port numbers, refer to “TCP/UDP port number ranges” (page 261).

| **port-name**  | Allows use of common names for certain well-known UDP port numbers. You can type in the specific name instead of having to recall the corresponding number:
|----------------|----------------------------------------------------------------------------------|
|                | - dns (Domain name service (53))
|                | - ntp (Network time protocol (123))
|                | - netbios-ns (NetBIOS name service (137))
|                | - netbios-dgm (NetBIOS datagram service (138))
|                | - radius (Remote authentication dial-in user service (1812))
|                | - radius-old (Remote authentication dial-in user service (1645))
|                | - rip (Routing information protocol (520))
|                | - snmp (Simple network management protocol (161))
|                | - snmp-trap (Simple network management protocol (162))
|                | - tftp (Trivial file transfer protocol (69))
|                | - timep (Time protocol (37))

**Example**

The following command configures the routing switch to forward UDP broadcasts from a client on VLAN 1 for a time protocol server:

```
HP Switch(vlan-1)# ip forward-protocol udp 15.75.11.155 timep
```

**Viewing the current IP forward-protocol configuration**

**Syntax:**

```
show ip forward-protocol [vlan vid]
```
Displays the current status of UDP broadcast forwarding and lists the UDP forwarding addresses configured on all static VLANS in the switch or on a specific VLAN.

*Example*

**Example 128 Displaying global IP forward-protocol status and configuration**

This example shows the global display showing UDP broadcast forwarding status and configured forwarding addresses for inbound UDP broadcast traffic for all VLANS configured on the routing switch.

```
HP Switch(config)# show ip forward-protocol

IP Forwarder Addresses

UDP Broadcast Forwarding: Disabled

VLAN: 1
IP Forward Addresses UDP Port
------------------------ --------
15.75.11.43          37
15.75.11.255         53
15.75.12.255         1813

VLAN: 2
IP Forward Addresses UDP Port
------------------------ --------
15.75.12.255         1812
```

**Example 129 Displaying IP forward-protocol status and per-VLAN configuration**

This example shows the display of UDP broadcast forwarding status and the configured forwarding addresses for inbound UDP broadcast traffic on VLAN 1.

```
HP Switch(config)# show ip forward-protocol vlan 1

IP Forwarder Addresses

UDP Broadcast Forwarding: Disabled

IP Forward Addresses UDP Port
------------------------ --------
15.75.11.43          37
15.75.11.255         53
15.75.12.255         1813
```

*Operating notes for UDP broadcast forwarding*

**Maximum number of entries**

The number of UDP broadcast entries and IP helper addresses combined can be up to 16 per VLAN, with an overall maximum of 2048 on the switch. (IP helper addresses are used with the switch’s DHCP relay operation.)

For example, if VLAN 1 has 2 IP helper addresses configured, you can add up to 14 UDP forwarding entries in the same VLAN.
TCP/UDP port number ranges

There are three ranges:

- Well-known ports: 0 to 1023
- Registered ports: 1024 to 49151
- Dynamic and/or private ports: 49152 to 65535

For more information, including a listing of UDP/TCP port numbers, go to the Internet Assigned Numbers Authority (IANA) website at:

www.iana.org

Then click on:

Protocol Number Assignment Services

P (Under "Directory of General Assigned Numbers" heading)

Port Numbers

Messages related to UDP broadcast forwarding

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp-bcast-forward: IP Routing support must be enabled first.</td>
<td>Appears in the CLI if an attempt to enable UDP broadcast forwarding has been made without IP routing being enabled first. Enable IP routing, then enable UDP broadcast forwarding.</td>
</tr>
<tr>
<td>UDP broadcast forwarder feature enabled</td>
<td>UDP broadcast forwarding has been globally enabled on the router. Appears in the Event Log and, if configured, in SNMP traps.</td>
</tr>
<tr>
<td>UDP broadcast forwarder feature disabled</td>
<td>UDP broadcast forwarding has been globally disabled on the routing switch. This action does not prevent you from configuring UDP broadcast forwarding addresses, but does prevent UDP broadcast forwarding operation. Appears in the Event Log and, if configured, in SNMP traps.</td>
</tr>
<tr>
<td>UDP broadcast forwarder must be disabled first.</td>
<td>Appears in the CLI if you attempt to disable routing while UDP forwarding is enabled on the switch.</td>
</tr>
</tbody>
</table>

UDP broadcast forwarding

Some applications rely on client requests sent as limited IP broadcasts addressed to a UDP application port. If a server for the application receives such a broadcast, the server can reply to the client. Since typical router behavior, by default, does not allow broadcast forwarding, a client’s UDP broadcast requests cannot reach a target server on a different subnet unless the router is configured to forward client UDP broadcasts to that server.

A switch with routing enabled includes optional per-VLAN UDP broadcast forwarding that allows up to 256 server and/or subnet entries on the switch (16 entries per-VLAN). If an entry for a particular UDP port number is configured on a VLAN, and an inbound UDP broadcast packet with that port number is received on the VLAN, the switch routes the packet to the appropriate subnet. (Each entry can designate either a single device or a single subnet. The switch ignores any entry that designates multiple subnets.)

**NOTE:** The number of UDP broadcast forwarding entries supported is affected by the number of IP helper addresses configured to support DHCP relay. See “Operating notes for UDP broadcast forwarding” (page 260).
A UDP forwarding entry includes the desired UDP port number and can be either an IP unicast address or an IP subnet broadcast address for the subnet the server is in. Thus, an incoming UDP packet carrying the configured port number will be:

- Forwarded to a specific host if a unicast server address is configured for that port number.
- Broadcast on the appropriate destination subnet if a subnet address is configured for that port number.

A UDP forwarding entry for a particular UDP port number is always configured in a specific VLAN and applies only to client UDP broadcast requests received inbound on that VLAN. If the VLAN includes multiple subnets, the entry applies to client broadcasts with that port number from any subnet in the VLAN.

For example, VLAN 1 (15.75.10.1) is configured to forward inbound UDP packets as shown in Table 40 (page 262).

### Table 40 Example of a UDP packet-forwarding environment

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP address</th>
<th>Subnet mMask</th>
<th>Forwarding address</th>
<th>UDP port</th>
<th>Notes</th>
</tr>
</thead>
</table>
| VLAN 1    | 15.75.10.1   | 255.255.255.0| 15.75.11.43, 15.75.11.255, 15.75.12.255 | 1188, 1812, 1813 | Unicast address for forwarding inbound UDP packets with UDP port 1188 to a specific device on VLAN 2.  
Broadcast address for forwarding inbound UDP packets with UDP port 1812 to any device in the 15.75.11.0 network.  
Broadcast address for forwarding inbound UDP packets with UDP port 1813 to any device in the 15.75.12.0 network. |
| VLAN 2    | 15.75.11.1   | 255.255.255.0| None               | N/A       | Destination VLAN for UDP 1188 broadcasts from clients on VLAN 1. The device identified in the unicast forwarding address configured in VLAN 1 must be on this VLAN.  
Also the destination VLAN for UDP 1812 from clients on VLAN 1. |
| VLAN 3    | 15.75.12.1   | 255.255.255.0| None               | N/A       | Destination VLAN for UDP 1813 broadcasts from clients on VLAN 1. |

**NOTE:** If an IP server or subnet entry is invalid, a switch will not try to forward UDP packets to the configured device or subnet address.

### Subnet masking for UDP forwarding addresses

The subnet mask for a UDP forwarding address is the same as the mask applied to the subnet on which the inbound UDP broadcast packet is received. To forward inbound UDP broadcast packets as limited broadcasts to other subnets, use the broadcast address that covers the subnet you want to reach. For example, if VLAN 1 has an IP address of 15.75.10.1/24 (15.75.10.1 255.255.255.0), you can configure the following unicast and limited broadcast addresses for UDP packet forwarding to subnet 15.75.11.0:

<table>
<thead>
<tr>
<th>Forwarding destination type</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP unicast to a single device in the 15.75.11.0 subnet</td>
<td>15.75.11.X</td>
</tr>
<tr>
<td>UDP broadcast to subnet 15.75.11.0</td>
<td>15.75.11.255</td>
</tr>
</tbody>
</table>
# 12 Virtual Router Redundancy Protocol (VRRP)

## Table 41 Summary of commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no]</code> router vrrp</td>
<td>Enables or disables VRRP operation in the global configuration context.</td>
<td>Disabled</td>
<td>(page 265)</td>
<td>-</td>
</tr>
<tr>
<td><code>[no]</code> router vrrp traps</td>
<td>Enables or disables SNMP trap generation.</td>
<td>Enabled</td>
<td>(page 265)</td>
<td>-</td>
</tr>
<tr>
<td><code>[no]</code> vrrp vrid 1-255</td>
<td>Used in the VLAN interface context to create a virtual router (VR) instance and to enter the context of the new VR.</td>
<td>-</td>
<td>(page 266)</td>
<td>-</td>
</tr>
<tr>
<td>[ owner</td>
<td>backup ]</td>
<td>Used in a VR context of a VLAN to set the router as either the owner of the VR on that interface or as a backup.</td>
<td>None</td>
<td>(page 266)</td>
</tr>
<tr>
<td>virtual-ip-address owner-ip-addr / mask-length virtual-ip-address owner-ip-addr mask</td>
<td>Used in a VR context of a VLAN to assign an IP address/mask combination to a VR instance.</td>
<td>None</td>
<td>(page 267)</td>
<td>-</td>
</tr>
<tr>
<td>priority 1 - 254</td>
<td>Changes the backup’s priority and is used to establish the precedence of a backup where there are multiple backups belonging to the same network or subnet.</td>
<td>100</td>
<td>(page 268)</td>
<td>-</td>
</tr>
<tr>
<td>advertise-interval 1-255</td>
<td>• When a VRRP router is operating as master, specifies the interval at which the router sends an advertisement notifying the other VRRP routers on the network or subnet that a master is active. • When a VRRP router is operating as a backup, it uses this value to calculate a timeout interval (3 x advt-interval).</td>
<td>1 second</td>
<td>(page 268)</td>
<td>-</td>
</tr>
<tr>
<td>primary-ip-address [ ip-address</td>
<td>lowest ]</td>
<td>Specifies the VIP to designate as the source for VRRP advertisements from the VR.</td>
<td>Lowest</td>
<td>(page 268)</td>
</tr>
<tr>
<td>[no] preempt-mode</td>
<td>Disables or re-enables preempt mode.</td>
<td>Enabled</td>
<td>(page 269)</td>
<td>-</td>
</tr>
<tr>
<td>[no] enable</td>
<td>After configuring a new VR or changing the configuration on an existing VR, you must use this command to enable the VR to operate.</td>
<td>Disabled</td>
<td>(page 269)</td>
<td>-</td>
</tr>
<tr>
<td>[no] track interface port-list/trunk-list</td>
<td>Allows you to specify a port or port list, or trunk or trunk list, that will be tracked by this virtual router.</td>
<td>-</td>
<td>(page 270)</td>
<td>-</td>
</tr>
<tr>
<td>[no] track vlan vlan-id range</td>
<td>Allows you to specify a VLAN or range of VLANs that will be tracked by this virtual router.</td>
<td>-</td>
<td>(page 270)</td>
<td>-</td>
</tr>
<tr>
<td>no track</td>
<td>Removes all interfaces and vlans from being tracked.</td>
<td>-</td>
<td>(page 271)</td>
<td>-</td>
</tr>
<tr>
<td>failover [with-monitoring]</td>
<td>Forces the backup VR operating as master to relinquish ownership of the VR instance.</td>
<td>-</td>
<td>(page 271)</td>
<td>-</td>
</tr>
<tr>
<td>failback</td>
<td>Forces the backup VR to take ownership of the VR instance.</td>
<td>-</td>
<td>(page 271)</td>
<td>-</td>
</tr>
<tr>
<td>[no] router vrrp virtual-ip-ping</td>
<td>Enables or disables the response to a ping request for the switch.</td>
<td>Response to virtual</td>
<td>(page 271)</td>
<td>-</td>
</tr>
</tbody>
</table>
Table 41 Summary of commands (continued)

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] virtual-ip-ping enabled</td>
<td>Enables or disables the response to a ping request to a specific VIP.</td>
<td>Enabled</td>
<td>(page 272)</td>
<td></td>
</tr>
<tr>
<td>show vrrp config global</td>
<td>Displays global VRRP configuration information.</td>
<td>-</td>
<td>(page 273)</td>
<td></td>
</tr>
<tr>
<td>[no] preempt-delay-time 1-600</td>
<td>Allows you to specify a time in seconds that this router will wait before taking control of the VIP and beginning to route packets.</td>
<td>zero seconds</td>
<td>(page 276)</td>
<td></td>
</tr>
<tr>
<td>show vrrp config global</td>
<td>Displays the configuration state for the global VRRP configuration and VRRP trap generation.</td>
<td>-</td>
<td>(page 276)</td>
<td></td>
</tr>
<tr>
<td>show vrrp config</td>
<td>Displays the configuration for the global VRRP configuration and all VRs configured on the router.</td>
<td>-</td>
<td>(page 277)</td>
<td></td>
</tr>
<tr>
<td>show vrrp vlan 23 vrid 10 config</td>
<td>Displays the configuration for a specific VR in a specific VLAN.</td>
<td>-</td>
<td>(page 278)</td>
<td></td>
</tr>
<tr>
<td>show vrrp statistics global</td>
<td>Displays the global VRRP statistics for the router.</td>
<td>-</td>
<td>(page 279)</td>
<td></td>
</tr>
<tr>
<td>show vrrp [statistics]</td>
<td>Displays statistics for all VRRP instances on the router.</td>
<td>-</td>
<td>(page 280)</td>
<td></td>
</tr>
<tr>
<td>show vrrp vlan vid [statistics]</td>
<td>Displays the VRRP statistics for all VRs configured on the specified VLAN.</td>
<td>-</td>
<td>(page 282)</td>
<td></td>
</tr>
<tr>
<td>show vrrp vlan vid vrid 1 - 255 [statistics]</td>
<td>Displays the VRRP statistics for a specific VR configured on a specific VLAN.</td>
<td>-</td>
<td>(page 283)</td>
<td></td>
</tr>
<tr>
<td>show vrrp</td>
<td>Displays the &quot;near-failovers&quot; statistic.</td>
<td>-</td>
<td>(page 283)</td>
<td></td>
</tr>
<tr>
<td>[no] debug vrrp</td>
<td>Displays VRRP debug messages.</td>
<td>-</td>
<td>(page 284)</td>
<td></td>
</tr>
</tbody>
</table>

**VRRP overview**

In many networks, edge devices are often configured to send packets to a statically configured default router. If this router becomes unavailable, the devices that use it as their first-hop router become isolated from the network. Virtual Router Redundancy Protocol (VRRP) uses dynamic failover to ensure the availability of an end node's default router. This is done by assigning the IP address used as the default route to a "virtual router" or VR. The VR includes:

- An owner router assigned to forward traffic designated for the virtual router (If the owner is forwarding traffic for the VR, it is the master router for that VR.)
- One or more prioritized backup routers (If a backup is forwarding traffic for the VR, it has replaced the owner as the master router for that VR.)

This redundancy provides a backup for gateway IP addresses (first-hop routers) so that if a VR's master router becomes unavailable, the traffic it supports will be transferred to a backup router without major delays or operator intervention. This operation can eliminate single-point-of-failure problems and provide dynamic failover (and failback) support. As long as one physical router in a VR configuration is available, the IP addresses assigned to the VR are always available, and the edge devices can send packets to these IP addresses without interruption.
Advantages to using VRRP include:
- Minimizing failover time and bandwidth overhead if a primary router becomes unavailable.
- Minimizing service disruptions during a failover.
- Providing backup for a load-balanced routing solution.
- Addressing failover problems at the router level instead of on the network edge.
- Avoiding the need to make configuration changes in the end nodes if a gateway router fails.
- Eliminating the need for router discovery protocols to support failover operation.

For more information, see “General operation” (page 284).

Configuring VRRP

Enabling VRRP in the global configuration context

VRRP can be configured regardless of the global VRRP configuration status. However, enabling a VR and running VRRP requires enabling it in the global configuration context.

Syntax:

```
[no] router vrrp
```

Enables or disables VRRP operation in the global configuration context. IP routing must be enabled before enabling VRRP on the router. Disabling global VRRP halts VRRP operation on the router, but does not affect the current VRRP configuration. Enabling or disabling VRRP generates an Event Log message.

To display the current global VRRP configuration, use `show vrrp config global`.

Default: Disabled

Syntax:

```
[no] router vrrp traps
```

Enables or disables SNMP trap generation for the following events:
- New master
  - Indicates that the sending router has transitioned to 'master' state.
- Authentication Failure
  - Indicates that a VRRP packet has been received from a router whose authentication key or authentication type conflicts with this router’s authentication key or authentication type.

**NOTE:** This feature assumes the `snmp-server host` command has been used to configure a a trap receiver. If a VRRP packet is received with an authentication type other than 0 (zero, that is, no authentication), the packet is dropped. See “Operating notes” (page 296).

Default: Enabled
Example

Example 130 Enabling and displaying the global VRRP configuration

The following commands enable VRRP at the global configuration level and then display the current global VRRP configuration:

HP Switch(config)# router vrrp
HP Switch(config)# show vrrp config global

VRRP Global Configuration Information

VRRP Enabled : Yes
Traps Enabled : Yes

Creating a VR and entering the VR context

Syntax:

\[
\text{[no]} \text{ vrrp vrid 1-255}
\]

Used in the VLAN interface context to create a virtual router (VR) instance and to enter the context of the new VR. It is also used to enter the context of an existing VR, and is the method used for accessing a VR for configuration purposes. You can configure up to 32 VRs on a multinetted VLAN.

The VLAN interface must be IP enabled.

Example

To create VR 1 in VLAN 10 and enter the VR context, execute the following command:

HP Switch(vlan-10)# vrrp vrid 1
HP Switch(vlan-10-vrid-1)#

Configuring a VR instance on a VLAN interface

This section describes the configuration and activation commands available in the VR context.

Assigning owner and backup status

Each VRRP router must be configured as either the owner of the VR instance or a backup for the instance.

Syntax:

\[ \text{[ owner | backup ]} \]

Used in a VR context of a VLAN to set the router as either the owner of the VR on that interface or as a backup. There can be one owner per network or subnet for a given VR.

If the VLAN is multinetted and multiple subnets are configured in the same VR, the router must be either the owner for all subnets in the VR or a backup for all subnets in the VR. The VR instance must be disabled (the default VR state) when using this command.

Default: None
Example

Example 131 Owner configuration on a VR

These commands configure and display the owner status in VR 1 on VLAN 10:

```
HP Switch(vlan-10-vrid-1)# owner
HP Switch(vlan-10-vrid-1)# show vrrp config
```

VRRP Global Configuration Information
VRRP Enabled : Yes
Traps Enabled : Yes

VRRP Virtual Router Configuration Information
Vlan ID : 10
Virtual Router ID : 10

Administrative Status [Disabled] : Disabled
Mode [Uninitialized] : owner
Priority [100] : 255
Advertisement Interval [1] : 1
Preempt Mode [True] : True
Primary IP Address : Lowest

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

Executing the `owner` or `backup` command must be done in the VR context of the VLAN in which the VR exists.

Mode and Priority settings for the configured owner on a VR.

---

Configuring a virtual IP address (VIP) in a VR

The VIP must be the same for the owner and all backups on the same network or subnet in a VR.

**Syntax:**

```
virtual-ip-address owner-ip-addr / mask-length
virtual-ip-address owner-ip-addr mask
```

Used in a VR context of a VLAN to assign an IP address/mask combination to a VR instance.

For an owner

- The VIP must be one of the IP addresses configured on the VLAN interface for that VR.

For a backup

- The VIP must match the VIP for the owner.

- The owner and the backups using a given VIP must all belong to the same network or subnet. Also, the VR instance must be disabled (the default VR state) when using this command.

Default: None

**Example**

If VLAN 10 on router "A" is configured with an IP address of 10.10.10.1/24 and VR 1, and you want router "A" to operate as the owner for this VR, the VIP of the owner in VR 1 on router "A" is also 10.10.10.1/24. On router "B," which will operate as a backup for VR 1, VLAN 10 is configured (in the same network) with an IP address of 10.10.10.15/24. However, because the backup must use the same VIP as the owner, the VIP for the backup configured on router "B" for VR 1 is also 10.10.10.1/24.
Reconfiguring the priority for a backup

When you configure a backup in a VR, it is given a default priority of 100. This command is intended for use where it is necessary to establish a precedence among the backup routers on the same network or subnet in a given VR.

Syntax:

```
priority 1-254
```

Used in a VR context of a VLAN where the router is configured as a backup. This command changes the backup’s priority and is used to establish the precedence of a backup where there are multiple backups belonging to the same network or subnet.

The VR instance must be disabled (the default VR state) when using this command.

NOTE: An owner is automatically assigned the highest priority, 255, which cannot be changed unless the owner status is reconfigured to backup.

Default: 100; Range: 1 - 254, where 1 is the lowest precedence

Changing VR advertisement interval and source IP address

Syntax:

```
advertise-interval 1-255
```

- When a VRRP router is operating as master, this value specifies the interval at which the router sends an advertisement notifying the other VRRP routers on the network or subnet that a master is active.
- When a VRRP router is operating as a backup, it uses this value to calculate a timeout interval (3 x advt-interval).

The VR instance must be disabled (the default VR state) when using this command.

Default: 1 second; range: 1–255 seconds

For information on advertisements and advertisement intervals, see “Function of the VRRP advertisement” (page 287).

NOTE: All VRRP routers belonging to the same VR must be configured with the same advertisement interval. As required in RFC 3768, if a locally configured advertisement interval does not match the interval received in an inbound VRRP packet, the VR drops that packet.
Syntax:

```plaintext
primary-ip-address [ ip-address | lowest ]
```

Specifies the VIP to designate as the source for VRRP advertisements from the VR. If there is only one VIP configured on the VR, the default setting (lowest) is sufficient. Where there are multiple VIPs in the same VR and you want to designate an advertisement source other than the lowest IP Address, use this command.

For an owner VR, the primary IP address must be one of the VIPs configured on the VR.

For a backup VR, the primary IP address must be in the same subnet as one of the VIPs configured on the VR. In addition, the primary IP address for a backup VR must be one of the IP addresses configured on the VLAN on which the VR is configured.

The VR instance must be disabled (the default VR state) when using this command.

Default: lowest

**NOTE:** It is common in VRRP applications to have only one VIP per VR. In such cases, the protocol uses that address as the source IP address for VRRP advertisements, and it is not necessary to specify an address.

### Configuring preempt mode on VRRP backup routers

This command applies to VRRP backup routers only and is used to minimize network disruption caused by unnecessary preemption of the master operation among backup routers.

**Syntax:**

```plaintext
[no] preempt-mode
```

Disables or re-enables preempt mode. In the default mode, a backup router coming up with a higher priority than another backup that is currently operating as master will take over the master function.

Using the `no` form of the command disables this operation, thus preventing the higher-priority backup from taking over the master operation from a lower-priority backup.

This command does not prevent an owner router from resuming the master function after recovering from being unavailable. The VR instance must be disabled (the default VR state) when using this command.

For more on preempt mode, see “Preempt mode” (page 288).

Default: Enabled

### Enabling or disabling VRRP operation on a VR

After configuring a new VR or changing the configuration on an existing VR, you must use this command to enable the VR to operate.

**Syntax:**

```plaintext
[no] enable
```

Enabling or disabling a VR enables or disables dynamic VRRP operation on that VR. Also, it is necessary to disable a VR before changing its configuration.

VRRP must be enabled (using the `router vrrp` command) in the global configuration context before enabling a VR. (Disabling a VR can be done regardless of the current, global VRRP configuration.)

Default: Disabled
Dynamically changing the priority of the VR

**NOTE:** You can configure only tracked interfaces or VLANs on the backup router.

Configuring track interface

**NOTE:** VR operation must be down before executing this command. Use the `no enable` command to disable VR operation.

**Syntax:**

```
[no] track interface port-list/trunk-list
```

Allows you to specify a port or port list, or trunk or trunk list, that will be tracked by this virtual router. If the port or trunk is down, the virtual router switches to the router specified by the priority value. The command is executed in VRID instance context.

**Example**

```
HP Switch(config)# vlan 25
HP Switch(vlan-25)# vrid 1
HP Switch(vlan-25-vrid-1)# track interface 10-12, Trk1
```

Configuring track VLAN

**NOTE:** VR operation must be down before executing this command. Use the `no enable` command to disable VR operation.

The VR's operating VLAN cannot be configured as a tracking VLAN for that VR.

**Syntax:**

```
[no] track vlan vlan-id range
```

Allows you to specify a VLAN or range of VLANs that will be tracked by this virtual router. If the VLAN is down, or if the VLAN or IP address has been deleted, the virtual router switches to the router specified by the priority value. The command is executed in VRID instance context.

**Example**

```
HP Switch(config)# vlan 25
HP Switch(vlan-25)# vrid 1
HP Switch(vlan-25-vrid-1)# track vlan 10 24-26
```

**NOTE:** When the first tracked port or tracked VLAN comes up after being down, the VR waits for the pre-empt delay time before it tries to take control back. The VR resumes being a backup with its configured priority as soon as the first tracked entity is up.

The behavior of the VR is not affected by any tracked entities until after the expiration of the preempt delay time. However, if while waiting for the preempt delay time to expire, a master goes down, the VR tries to take control of the virtual IP.
Removing all tracked entities

**Syntax:**

```no track```

Allows you to remove tracking for all configured track entities (ports, trunks, and VLANs). The command is executed in VRID instance context.

**Example**

```
HP Switch(vlan-25-vrid-1)# no track
```

Forcing the backup VR operating as master to relinquish ownership of the VR instance

**Syntax:**

```failover [with-monitoring]```

The command is executed in VRID instance context

Forcing the backup VR to take ownership of the VR instance

Failback is disabled on the owner VR; it can be executed only on the backup VR. Failback can occur only on a VR on which `failover` or `failover with-monitoring` has been executed.

**Syntax:**

```failback```

This command takes effect only if the backup VR instance has a higher priority than the current owner, which is normal VRRP router behavior. The command is executed in VRID instance context.

Viewing VRRP tracked entities

You can display the VRRP tracked entities by entering the command shown in this example.

**Example 132 Example showing results of show vrrp tracked entities command**

```
HP Switch(vlan-25-vrid-1)# show vrrp tracked-entities
```

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>VR ID</th>
<th>Type</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>1</td>
<td>port</td>
<td>7</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>port</td>
<td>12</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>port</td>
<td>13</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>port</td>
<td>14</td>
</tr>
<tr>
<td>25</td>
<td>1</td>
<td>vlan</td>
<td>1</td>
</tr>
</tbody>
</table>

Pinging the virtual IP of a backup router

For more information, see “Pinging the virtual IP of a backup router” (page 293).

Enabling the response to a ping request

The backup router can be enabled to respond to pings using the following command. For more information, see “Pinging the virtual IP of a backup router” (page 293).
**Syntax:**

```
[no] router vrrp virtual-ip-ping
```

Enables or disables the response to a ping request for the switch. When enabled, all VRs that are not owners and are not explicitly disabled (see `virtual-ip-ping enabled` command) respond to ping requests sent to the VIP when the backup VR is acting as master.

Default: Response to virtual IP ping is disabled.

**Example**

**Example 133 Enabling the response to ping requests**

```bash
HP-Router1# config
HP-Router1(config)# ip routing
HP-Router1(config)# router vrrp
HP-Router1(config)# router vrrp virtual-ip-ping
```

**Controlling ping responses**

This feature, which is a change in configuration, can only be enabled or disabled when the VR is disabled.

**Syntax:**

```
[no] virtual-ip-ping enabled
```

Enables or disables the response to a ping request to a specific VIP. The command applies to all VIPs on the VR.

Must be executed in VRRP context (`vlan vid vrrp vrid vrid`)

**NOTE:** The VR should be configured as a backup.

Default: Enabled
**Example**

**Example 134 Disabling a response to ping requests to a VIP**

<table>
<thead>
<tr>
<th>HP Switch-Router1(config)# ip routing</th>
<th>Enable routing</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Switch-Router1(config)# router vrrp</td>
<td>Enable VRRP</td>
</tr>
<tr>
<td>HP Switch-Router1(config)# router vrrp virtual-ip-ping</td>
<td>Enable response to ping request</td>
</tr>
<tr>
<td>HP Switch-Router1(config)# vlan 2 vrrp vrid 1</td>
<td>Enter VLAN context and configure a VR instance</td>
</tr>
<tr>
<td>HP Switch-Router1(vlan-2-vrid-1)# backup</td>
<td>Configure the router as backup</td>
</tr>
<tr>
<td>HP Switch-Router1(vlan-2-vrid-1)# virtual-ip-address 10.0.202.87/32</td>
<td>Configure Virtual IP address for VR instance</td>
</tr>
<tr>
<td>HP Switch-Router1(vlan-2-vrid-1)# no virtual-ip-ping enable</td>
<td>Disable the response to a ping request to all the Virtual IP addresses for this VR</td>
</tr>
<tr>
<td>HP Switch-Router1(vlan-2-vrid-1)# enable</td>
<td>Activate VR instance</td>
</tr>
<tr>
<td>HP Switch-Router1(vlan-2-vrid-1)# exit</td>
<td>Exit to vlan context.</td>
</tr>
<tr>
<td>HP Switch-Router1(vlan-2-vrid-1)# exit</td>
<td>Exit to config context.</td>
</tr>
<tr>
<td>HP Switch-Router1(config)#</td>
<td></td>
</tr>
</tbody>
</table>

**Viewing VRRP ping information**

Display global VRRP configuration information by entering the `show vrrp config global` command.

**Example 135 Example of VRRP global configuration information**

<table>
<thead>
<tr>
<th>HP Switch(config)# show vrrp config global</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP Global Configuration Information</td>
</tr>
<tr>
<td>VRRP Enabled : Yes</td>
</tr>
<tr>
<td>Traps Enabled : Yes</td>
</tr>
<tr>
<td>Virtual Routers Respond to Ping Requests [Yes] : Yes</td>
</tr>
</tbody>
</table>

Use the `show vrrp` command to display information about VRRP global statistics.
Display VRRP configuration information using the `show vrrp config` command.
**Example 137 Example of VRRP configuration display showing VIP ping status**

```
HP Switch-Router1(config)# show vrrp config

VRRP Global Configuration Information

VRRP Enabled : Yes
Traps Enabled : Yes
Virtual Routers Respond to Ping Requests : Yes

VRRP Virtual Router Configuration Information

Vlan ID : 2
Virtual Router ID : 1

Administrative Status [Disabled] : Enabled
Mode [Uninitialized] : backup
Priority [100] : 150
Advertisement Interval [1] : 1
Preempt Mode [True] : True
Preempt delay time : 0
Respond to Virtual IP Ping Requests [Yes] : Yes
Primary IP Address : Lowest

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.202.87</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>
```

**Example 138 Example of VRRP configuration for a VLAN and VRID**

This example displays the ping response status for a specific VLAN and VRID.

```
HP Switch-Router1(config)# show vrrp vlan 2 vrid 1 config

VRRP Virtual Router Configuration Information

Vlan ID : 2
Virtual Router ID : 1

Administrative Status [Disabled] : Enabled
Mode [Uninitialized] : backup
Priority [100] : 150
Advertisement Interval [1] : 1
Preempt Mode [True] : True
Preempt delay time : 0
Respond to Virtual IP Ping Requests [Yes] : Yes
Primary IP Address : Lowest

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.202.87</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>
```

**Example 139 Example of IP route information**

This example shows the gateway information for IP routes. A designation of "reject" means that the IP traffic for that route is discarded. For VIP entries, when the backup ping feature is enabled, no ping error messages are sent for the discarded packets.

```
HP Switch(config)# show ip route

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>DEFAULT_VLAN</td>
<td>1</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>10.0.202.87/32</td>
<td>reject</td>
<td>1</td>
<td>static</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td>1</td>
<td>static</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td>1</td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Ringing the virtual IP of a backup router
Operational notes

- Jumbo frames are supported if they have been enabled for that VLAN. The VIP responds to ping requests if they are not fragmented and are not larger than the MTU.
- Fragmented packets are not supported. All fragmented packets sent to a VIP are dropped and no response or error is sent.
- All packets with IP options are dropped. Any ping options will work as long as they do not change to IP options.
- ICMP requests other than echo requests are not supported.
- If there are errors in packets sent to a VIP, for example, “TTL Invalid,” no ICMP error packet is sent.

Specifying the time a router waits before taking control of the VIP

For more information, see “Using the Pre-empt Delay Timer” (page 294).

Syntax:

```bash
[no] preempt-delay-time 1-600
```

Allows you to specify a time in seconds that this router will wait before taking control of the VIP and beginning to route packets. You can configure the timer on VRRP owner and backup routers.

**NOTE:** If you have configured the preempt delay time (PDT) with a non-zero value, you must use the `no` form of the command to change it to 0 (zero).

Default: 0 (zero) seconds.

**NOTE:** The value of the PDT cannot be changed when the VR is active. This is in accordance with other VR parameters (such as advertisement interval, priority, VIP, mode, and so forth) that cannot be changed when the VR is active.

Viewing VRRP configuration data

Viewing the VRRP global configuration

Syntax:

```bash
show vrrp config global
```

Displays the configuration state for the global VRRP configuration and VRRP trap generation.
Example

Example 140 Output showing the default global VRRP configuration

HP Switch(config)# show vrrp config global

VRRP Global Configuration Information

- VRRP Enabled : No
- Traps Enabled : Yes

Viewing all VR configurations on the router

Syntax:

```
show vrrp config
```

Displays the configuration for the global VRRP configuration and all VRs configured on the router.
### Example 141 VRRP configuration listing with two owner VRs configured

This example lists output indicating two owner VRs configured on the router.

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

VRRP Global Configuration Information

  VRRP Enabled   : Yes
  Traps Enabled  : Yes

VRRP Virtual Router Configuration Information

  Vlan ID : 10
  Virtual Router ID : 10

  Administrative Status [Disabled] : Disabled
  Mode [Uninitialized] : owner
  Priority [100] : 255
  Advertisement Interval [1] : 1
  Preempt Mode [True] : True
  Primary IP Address : Lowest

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

VRRP Virtual Router Configuration Information

  Vlan ID : 20
  Virtual Router ID : 20

  Administrative Status [Disabled] : Enabled
  Mode [Uninitialized] : owner
  Priority [100] : 255
  Advertisement Interval [1] : 1
  Preempt Mode [True] : True
  Primary IP Address : Lowest

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.20.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>
```

This data shows the virtual IP address(es) configured on VR 10.

This data shows the virtual IP address(es) configured on VR 20.

---

### Viewing a specific VR configuration

**Syntax:**

```
show vrrp vlan 23 vrid 10 config
```

Displays the configuration for a specific VR in a specific VLAN.
**Example**

**Example 142 Displaying the configuration for a specific VR**

The following command displays the configuration of a VR identified as VR 10 in VLAN 23:

HP Switch(config)# show vrrp vlan 23 vrid 10 config

VRRP Virtual Router Configuration Information

<table>
<thead>
<tr>
<th>Vlan ID</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Router ID</td>
<td>10</td>
</tr>
<tr>
<td>Administrative Status [Disabled]</td>
<td>Disabled</td>
</tr>
<tr>
<td>Mode [Uninitialized]</td>
<td>Owner</td>
</tr>
<tr>
<td>Priority [100]</td>
<td>255</td>
</tr>
<tr>
<td>Advertisement Interval [1]</td>
<td>1</td>
</tr>
<tr>
<td>Preempt Mode [True]</td>
<td>True</td>
</tr>
<tr>
<td>Primary IP Address</td>
<td>Lowest</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Subnet Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

**Viewing VRRP statistics data**

All command outputs shown in this section assume that VRRP is enabled at the global configuration level. If global VRRP is disabled, these commands produce the following output:

**Example 143 statistics command output if global VRRP is disabled**

VRRP Global Statistics Information

| VRRP Enabled | : No |

**Viewing global VRRP statistics only**

**Syntax:**

show vrrp statistics global

Displays the global VRRP statistics for the router:

- VRRP Enabled
- Protocol Version: 2
- Invalid VRID Pkts Rx: VRRP packets received for a VRID that is not configured on the specific VLAN of the VRRP router.
- Checksum Error Pkts Rx: VRRP packets received with a bad checksum
- Bad Version Pkts Rx: VRRP advertisement packets received with a version number other than 2.
Example 144 Example of a global VRRP statistics output

HP Switch(config)# show vrrp statistics global

VRRP Global Statistics Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>2</td>
</tr>
<tr>
<td>Invalid VRID Pkts Rx</td>
<td>0</td>
</tr>
<tr>
<td>Checksum Error Pkts Rx</td>
<td>0</td>
</tr>
<tr>
<td>Bad Version Pkts Rx</td>
<td>0</td>
</tr>
</tbody>
</table>

Viewing statistics for all VRRP instances on the router

**Syntax:**

```
show vrrp [statistics]
```

Displays the following VRRP statistics:

- Global VRRP statistics for the router
- VRRP statistics for all VRs configured on the router:

**State**

Indicates whether the router is a backup or the current master of the VR.

**Uptime**

The amount of time the router has been up since the last reboot.

**Virtual MAC Address**

The virtual MAC address for the VR instance.

**master’s IP Address**

The IP address used as the source IP address in the last advertisement packet received from the VR master. If this VR is the master, this is the primary IP address of the VR. If the VR is disabled, this value appears as 0.0.0.0.

**Associated IP Address Count**

Number of VIPs.

**Advertise Packets Rx**

The number of VRRP master advertisements the VR has received from other VRRP routers since the last reboot.

**Zero Priority Tx**

The number of VRRP advertisement packets received with the priority field set to 0 (zero).

**Bad Length Pkts**

The number of VRRP packets received with missing fields of information.

**Mismatched Interval Pkts**

The number of VRRP packets received from other routers (since the last reboot) with an advertisement interval that is different from the interval configured on the current VR.

**Mismatched IP TTL Pkts**

The number of VRRP packets received with an interval mismatch are dropped.
Near Failovers
Tracks the occurrence of “near failovers” on the backup VRRP routers. This makes visible any difficulties the VRRP routers are having receiving the “heartbeat” advertisement from the master router. A "near failover" is one that is within one missed VRRP advertisement packet of beginning the master determination process.

Become master
The number of times the VR has become the master since the last reboot.

Zero Priority Tx
The number of VRRP advertisement packets sent with the priority field set to 0 (zero).

Bad Type Pkts
The number of VRRP packets received with packet type not equal to 1 (that is, not an advertisement packet).

Mismatched Addr List Pkts
The number of VRRP packets received wherein the list of VIPs does not match the locally configured VIPs for a VR.

Mismatched Auth Type Pkts
The number of VRRP packets received with the authentication type not equal to 0 (zero, which is no authentication).

Note that show vrrp and show vrrp statistics give the same output.
Example

Example 145 Output for show vrrp command includes global and VR statistics

The following output shows the VRRP statistics on a router having one VR (VR 1 in VLAN 10) configured.

HP Switch(config)# show vrrp

VRRP Global Statistics Information

VRRP Enabled : Yes
Protocol Version : 2
Invalid VRID Pkts Rx : 0
Checksum Error Pkts Rx : 0
Bad Version Pkts Rx : 0

VRRP Virtual Router Statistics Information

Vlan ID : 10
Virtual Router ID : 1
State : Master
Up Time : 31 mins
Virtual MAC Address : 00005e-000101
Master's IP Address : 10.10.10.2
Associated IP Addr Count : 1
Advertisement Pkts Rx : 1213
Zero Priority Rx : 0
Bad Length Pkts : 0
Mismatched Interval Pkts : 0
Mismatched IP TTL Pkts : 0
Near Failovers : 0
Become Master : 2
Zero Priority Tx : 0
Bad Type Pkts : 0
Mismatched Addr List Pkts : 0
Mismatched Auth Type Pkts : 0

Viewing statistics for all VRRP instances in a VLAN

Syntax:

```
show vrrp vlan vid [statistics]
```

Displays the VRRP statistics for all VRs configured on the specified VLAN.

The actual statistics data per VR is the same as for the show vrrp [statistics] command shown on pages A-24 and Example 145 (page 282).

Note that show vrrp vlan vid and show vrrp vlan vid statistics produce the same output.
Example

Example 146 Displaying statistics for all VRs in a VLAN

In the following example, there is one VR configured in VLAN 10.

HP Switch(config)# show vrrp vlan 10

VRRP Virtual Router Statistics Information

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan ID</td>
<td>10</td>
</tr>
<tr>
<td>Virtual Router ID</td>
<td>10</td>
</tr>
<tr>
<td>State</td>
<td>Master</td>
</tr>
<tr>
<td>Up Time</td>
<td>6 mins</td>
</tr>
<tr>
<td>Virtual MAC Address</td>
<td>00005e-00010a</td>
</tr>
<tr>
<td>Master's IP Address</td>
<td>10.10.10.1</td>
</tr>
<tr>
<td>Associated IP Addr Count</td>
<td>1</td>
</tr>
<tr>
<td>Near Failovers</td>
<td>0</td>
</tr>
<tr>
<td>Advertise Pkts Rx</td>
<td>1</td>
</tr>
<tr>
<td>Become Master</td>
<td>1</td>
</tr>
<tr>
<td>Zero Priority Rx</td>
<td>0</td>
</tr>
<tr>
<td>Zero Priority Tx</td>
<td>0</td>
</tr>
<tr>
<td>Bad Length Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Bad Type Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Mismatched Interval Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Mismatched Addr List Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Mismatched IP TTL Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Mismatched Auth Type Pkts</td>
<td>0</td>
</tr>
</tbody>
</table>

Viewing statistics for a specific VRRP instance

Syntax:

```
show vrrp vlan vid vrid 1-255 [statistics]
```

Displays the VRRP statistics for a specific VR configured on a specific VLAN.

The actual statistics data per VR is the same as for the `show vrrp [statistics]` command shown on pages A-24 and Example 145 (page 282).

Note that `show vrrp vlan vid vrid 1 - 255` and `show vrrp vlan vid vrid 1 - 255 statistics` produce the same output.

Viewing the "near-failovers" statistic

The "near-failovers" statistic tracks occurrences of near failovers on the backup VRRP routers. This makes visible any difficulties the VRRP routers are having receiving the "heartbeat" advertisement from the master router. (A "near failover" is one that is within one missed VRRP advertisement packet of beginning the master determination process.)

The `show vrrp` command displays this statistic.
Example 147 The show vrrp command with statistics

Near Failovers statistic displayed is shown in bold below.

HP Switch(config)# show vrrp

VRRP Global Statistics Information

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRRP Enabled</td>
<td>Yes</td>
</tr>
<tr>
<td>Protocol Version</td>
<td>2</td>
</tr>
<tr>
<td>Invalid VRID Pkts Rx</td>
<td>0</td>
</tr>
<tr>
<td>Checksum Error Pkts Rx</td>
<td>0</td>
</tr>
<tr>
<td>Bad Version Pkts Rx</td>
<td>0</td>
</tr>
</tbody>
</table>

VRRP Virtual Router Statistics Information

<table>
<thead>
<tr>
<th>Statistics</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan ID</td>
<td>22</td>
</tr>
<tr>
<td>Virtual Router ID</td>
<td>1</td>
</tr>
<tr>
<td>State</td>
<td>Initialize</td>
</tr>
<tr>
<td>Up Time</td>
<td>64 mins</td>
</tr>
<tr>
<td>Virtual MAC Address</td>
<td>00005e-000101</td>
</tr>
<tr>
<td>Master's IP Address</td>
<td></td>
</tr>
<tr>
<td>Associated IP Addr Count</td>
<td>1</td>
</tr>
<tr>
<td>Advertise Pkts Rx</td>
<td>0</td>
</tr>
<tr>
<td>Zero Priority Rx</td>
<td>0</td>
</tr>
<tr>
<td>Bad Length Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Mismatched Interval Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Mismatched IP TTL Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Near Failovers</td>
<td>0</td>
</tr>
<tr>
<td>Become Master</td>
<td>0</td>
</tr>
<tr>
<td>Zero Priority Tx</td>
<td>0</td>
</tr>
<tr>
<td>Bad Type Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Mismatched Addr List Pkts</td>
<td>0</td>
</tr>
<tr>
<td>Mismatched Auth Type Pkts</td>
<td>0</td>
</tr>
</tbody>
</table>

Using the debug command with the VRRP option

The vrrp option with the debug command turns on the tracing of the incoming and outgoing VRRP packets.

Syntax:

```
[no] debug vrrp
```

Displays VRRP debug messages.

General operation

License requirements:

In the 3500yl, 5400zl, and 6600 switches, VRRP is included with the Premium License. In the 6200yl and 8200zl switches, this feature is included with the base feature set.

VRRP supports router redundancy through a prioritized election process among routers configured as members of the same virtual router (VR).

On a given VLAN, a VR includes two or more member routers configured with a VIP that is also configured as a real IP address on one of the routers, plus a virtual router MAC address. The router that owns the IP address is configured to operate as the owner of the VR for traffic-forwarding purposes and by default has the highest VRRP priority in the VR. The other routers in the VR have a lower priority and are configured to operate as backups in case the owner router becomes unavailable.

The owner normally operates as the master for a VR. But if it becomes unavailable, then a failover to a backup router belonging to the same VR occurs, and this backup becomes the current master. If the owner recovers, a failback occurs and "master" status reverts to the owner.
one backup provides additional redundancy" if both the owner and the highest-priority backup fail, another, lower-priority backup can take over as master.)

**NOTE:**

- The VIP used by all VRRP routers in a VR instance is a real IP address that is also configured on the applicable VLAN interface on the VR's owner router.
- The same MAC and VIPs are included in the VRRP configuration for the owner and all backup routers belonging to the same VR and are used as the source addresses for all traffic forwarded by the VR.

Figure 45 (page 285) shows a VR on VLAN 100 supported by Router 1 (R1) and Router 2 (R2).

**Figure 45 Example of using VRRP to provide redundant network access**

<table>
<thead>
<tr>
<th>VR parameter</th>
<th>Router 1 VR configuration</th>
<th>Router 2 VR configuration</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRID (Virtual Router ID)</td>
<td>1</td>
<td>1</td>
<td>All routers in the same VR have the same VRID.</td>
</tr>
<tr>
<td>Status</td>
<td>owner</td>
<td>backup</td>
<td>One owner and one or more backups are allowed in a given VR.</td>
</tr>
<tr>
<td>Virtual IP Address</td>
<td>10.10.100.1</td>
<td>10.10.100.1</td>
<td>The IP address configured for VLAN 100 in R1 (the owner) is also configured as the VIP for VRRP in both R1 and R2.</td>
</tr>
<tr>
<td>VR Source MAC Address</td>
<td>00-00-5E-00-01-01</td>
<td></td>
<td>For any VR in any VLAN, this is always defined as 00-00-5E-00-01-VRID and is not configurable.</td>
</tr>
<tr>
<td>Priority</td>
<td>255 (Default)</td>
<td>100 (Default)</td>
<td>The router configured as owner in any VR is automatically assigned the highest priority (255); backup routers are assigned a default priority of 100, which can be reconfigured.</td>
</tr>
</tbody>
</table>
In Figure 45 (page 285):

- Host "A" uses 10.10.100.1 as its next-hop gateway out of the subnet, as represented by the VR (VR 1).
  - Router 1 (the configured owner) advertises itself as the master in the VR supporting the gateway and:
    - "Owns" the VR’s (virtual) IP address
    - Transmits ARP responses that associate the VR’s VIP with the (shared) source MAC address for VR 1.
  - During normal operation, Router 1 forwards the routed traffic for host "A."
- If Router 1 fails or otherwise becomes unavailable:
  a. Router 1 advertisements of its master status for VR 1 fail to reach Router 2 (which is the only configured backup).
  b. After the time-out period for receiving master advertisements expires on Router 2, the VR initiates a failover to Router 2 and it becomes the new master of the VR.
  c. Router 2 advertises itself as the master of the VR supporting the gateway and:
    - Takes control of the VR’s (virtual) IP address
    - Begins transmitting ARP responses that associate the VR’s VIP with the (shared) source MAC address for VR 1
  d. Host "A" routed traffic then moves through Router 2.
- If Router 1 again becomes available:
  a. Router 1 resumes advertising itself as the master for the VR and sends ARP responses that associate the VR’s VIP with the (shared) source MAC address for VR 1.
  b. Router 2 receives the advertisement from Router 1 and ceases to operate as the VR’s master, and halts further transmission of its own VRRP advertisements and ARP responses related to VR 1.
  c. The VR executes a failback to Router 1 as master, and Host "A" traffic again moves through Router 1.

Virtual router (VR)

A VR instance consists of one owner router and one or more backup routers belonging to the same network. Any VR instance exists within a specific VLAN, and all members of a given VR must belong to the same subnet. In a multinetted VLAN, multiple VRs can be configured. The owner operates as the VR’s master unless it becomes unavailable, in which case the highest-priority backup becomes the VR’s master.

A VR includes the following:
- VR identification (VRID) configured on all VRRP routers in the same network or, in the case of a multinetted VLAN, on all routers in the same subnet.
- Same VIP configured on each instance of the same VR.
- Status of either owner or backup configured on each instance of the same VR (on a given VR, there can be one owner and one or more backups).
- Priority level configured on each instance of the VR (on the owner router the highest priority setting, 255, is automatically fixed; on backups, the default priority setting is 100 and is configurable).
- VR MAC address (not configurable).

Where a VLAN is configured with only one network (IP address), one VR is allowed in that VLAN. In a multinetted VLAN, there can be one VR per subnet, with a maximum of 32 VRs in any combination of masters and backups.
NOTE: All routers in a given VR must belong to the same network (or subnet, in the case of a multinetted VLAN).

Virtual IP address (VIP)
The VIP associated with a VR must be a real IP address already configured in the associated VLAN interface on the owner router in the VR. Also, the owner and all other (backup) routers belonging to the VR have this IP address configured in their VRID contexts as the VIP. In Figure 45 (page 285), 10.10.100.1 is a real IP address configured on VLAN 100 in Router 1 and is the VIP associated with VR 1.

If the configured owner in a VR becomes unavailable, it is no longer the master for the VR and a backup router in the VR is elected to assume the role of master, as described under “Backup router” (page 288).

A subnetted VLAN allows multiple VIPs. However, if there are 32 or fewer IP addresses in a VLAN interface, and you want VRRP support on multiple subnets, the recommended approach is to configure a separate VR instance for each IP address in the VLAN. In cases where VRRP support is needed for more than 32 IP addresses in the same VLAN, see “Associating more than one VIP with a VR” (page 292).

Master router
The current master router in a VR operates as the "real" or physical gateway router for the network or subnet for which a VIP is configured.

Control of master selection
Selection of the master is controlled by the VRRP priority value configured in the VRID context of each router in the VR. The router configured as the owner in the VR is automatically assigned the highest VRRP priority (255) and, as long as it remains available, operates as the master router for the VR. The other routers belonging to the VR as backups are assigned the default priority value (100) and can be reconfigured to any priority value between 1 and 254, inclusive. If the current master becomes unavailable, the protocol uses the priority values configured on the other, available routers in the VR to select another router in the VR to take over the master function.

Function of the VRRP advertisement
The current master router sends periodic advertisements to inform the other routers in the VR of its operational status. If the backup VRs fail to receive a master advertisement within the timeout interval, the current master is assumed to be unavailable and a new master is elected from the existing backups. The timeout interval for a VR is three times the advertisement interval configured on the VRs in the network or subnet. In the default VRRP configuration, the advertisement interval is one second and the resulting timeout interval is three seconds.

NOTE: All VRRP routers belonging to the same VR must be configured with the same advertisement interval. As required in RFC 3768, if a locally configured advertisement interval does not match the interval received in an inbound VRRP packet, the VR drops that packet.

Owner router
An owner router for a VR is the default master router for the VR and operates as the owner for all subnets included in the VR. The VRRP priority on an owner router is always 255 (the highest).

NOTE: On a multinetted VLAN where multiple subnets are configured in the same VR, the router must be either the owner for all subnets in the VR or a backup for all subnets in the VR.
Backup router

There must be at least one backup router. A given VR instance on a backup router must be configured with the same VIP as the owner for that VR (and both routers must belong to the same network or subnet). Router 2 in Figure 45 (page 285) illustrates this point.

VR priority operation

In a backup router's VR configuration, the virtual router priority defaults to 100. (The priority for the configured owner is automatically set to the highest value: 255.) In a VR where there are two or more backup routers, the priority settings can be reconfigured to define the order in which backups are reassigned as master in the event of a failover from the owner.

Preempt mode

Where multiple backup routers exist in a VR, if the current master fails and the highest-priority backup is not available, VRRP selects the next-highest priority backup to operate as master. If the highest-priority backup later becomes available, it preempts the lower-priority backup and takes over the master function. If you do not want a backup router to have this preemptive ability on a particular VR, you can disable this operation with the no preempt-mode command. (Preempt mode applies only to VRRP routers configured as backups.) See “Configuring preempt mode on VRRP backup routers” (page 269).

Virtual router MAC address

When a VR instance is configured, the protocol automatically assigns a MAC address based on the standard MAC prefix for VRRP packets, plus the VRID number (as described in RFC 3768). The first five octets form the standard MAC prefix for VRRP, and the last octet is the configured VRID. that is:

```
00-00-5E-00-01-VRid
```

For example, the virtual router MAC address for the VR in Figure 45 (page 285) is 00-00-5E-00-01-01.

VRRP and ARP

The master for a given VR responds to ARP requests for the VIPs with the VR's assigned MAC address. The virtual MAC address is also used as the source MAC address for the periodic advertisements sent by the current master.

The VRRP router responds to ARP requests for non-VIPs (IP addresses on a VLAN interface that are not configured as VIPs for any VR on that VLAN) with the system MAC address.

General operating rules

- IP routing must be enabled on the router before enabling VRRP.
- IP must be enabled on a VLAN before creating a VR instance on the VLAN.
- VIP:
  - On an owner: The VIP configured in a VR instance must match one of the IP addresses configured in the VLAN interface on which the VR is configured.
  - On a backup: The VIP configured in a VR instance cannot be a "real" IP address configured in a VLAN interface on that router.
The VIP configured for one VR cannot be configured on another VR.

- Before changing a router from owner to backup, or the reverse, the VIP must be removed from the configuration.
- The priority configuration on an owner can be only 255. The priority configuration on a backup must be 254 or lower, the default being 100.
- Advertisement intervals:
  - A VRRP router must be configured as an owner or backup before configuring the advertisement interval.
  - If a VRRP router has a different advertisement interval than a VRRP packet it receives, the router drops the packet. For this reason, the advertisement interval must be the same for the owner and all backups in the same VR.
- When a VR is active you cannot change any of the following on that VR:
  - Priority
  - Advertisement interval
  - Preempt mode
  - VIP
- A VR exists within a single VLAN interface. If the VLAN is multinetted, a separate VR can be configured within the VLAN for each subnet. A VLAN allows up to 32 VRs, and the switch allows up to 2048 VRs.
- All routers in the same VR must belong to the same network or subnet.
- The router supports the following maximums:
  - 32 VRs per VLAN in any combination of masters and backups
  - 2048 VRs per router
  - 32 IP addresses per VR
- Each VR uses one MAC address as described under “Virtual router MAC address” (page 288).
- If an IP address is deleted on a VLAN interface, one of the following occurs:
  - VR owner: If the VR uses the same IP address as a VIP, that IP address is deleted from the VR.
  - VR backup: If the VR has a VIP in the same subnet as that of the deleted IP address, that VIP will be deleted from the VR.
  - If the deleted VIP was the last VIP of an active VR, the VR will be deactivated. (For more on multiple, VIPs on a VR, see “Associating more than one VIP with a VR” (page 292).
- The VRRP backup router can respond to ping requests when the virtual-ip-ping feature is enabled. For more information about this feature, see “Pinging the virtual IP of a backup router” (page 293).

Steps for provisioning VRRP operation

Basic configuration process

This process assumes the following for VRRP operation:
- VLANs on the selected routers are already configured and IP-enabled.
- IP routing is enabled.
- The network topology allows multiple paths for routed traffic between edge devices.
1. Configure the owner for VRRP operation and a VR instance.
   a. On the router intended as the owner for a particular network or subnet, enter the global
      configuration context and enable VRRP:
      
      ```
      router vrrp
      ```
   b. Enter the desired VLAN context and configure a VR instance:
      
      ```
      vlan  vid
      vrrp vrid 1 - 255
      ```
      This step places the CLI in the context of the specified VR.
   c. Configure the router as the owner of the VR instance:
      
      ```
      owner
      ```
      This step automatically fixes the router’s priority as 255 (the highest) for this VR instance. 
      (The owner priority cannot change.)
   d. Configure the router’s real IP address and subnet mask for the current VLAN interface as 
      the VIP for the VR instance. You can use either of the following methods:
      
      ```
      virtual-ip-address ipaddr mask
      virtual-ip-address ipaddr /mask-length
      ```
   e. Activate the owner VR instance:
      
      ```
      enable
      ```
   f. Inspect the configuration for the owner VR:
      
      ```
      show vrrp vlan vid vrid vrid-# config
      ```
      Leave the owner’s advertisement interval at its default (1 second). For more on this topic, see 
      “Changing VR advertisement interval and source IP address” (page 268).

2. Configure a backup for the same VR instance as for the owner in step 1 (page 290).
   a. On another router with an interface in the same network or subnet as is the owner 
      configured in step “1” (page 290), enter the global configuration context and enable VRRP:
      
      ```
      router vrrp
      ```
   b. Configure (and enter) the same VR instance as was configured for the owner in step 
      “1” (page 290):
      
      ```
      vlan  vid
      vrrp vrid 1 - 255
      ```
   c. Configure the router as a backup for the VR instance:
      
      ```
      backup
      ```
      This step sets the backup router’s priority as 100 for this VR instance.
   d. Optional: If there is only one backup router, or if you want the priority among backups 
      to be determined by the lowest IP address among the backups, leave the VR instance 
      priority for the current backup router at the default of 100. (Applies only to the "real" IP 
      addresses that are part of this VR—there may be other addresses on the routers that are lower—but only the interfaces participating in the VR are part of this determination). If 
      you want to control backup router priority by creating a numeric hierarchy among the 
      backup routers in the VR, set the priority on each accordingly:
      
      ```
      priority 1 - 254
      ```
   e. Configure the VIP for the current VR. Use the same address as you used for the owner 
      router’s instance of the VR. You can use either of the following methods:
      
      ```
      virtual-ip-address ipaddr mask
      ```
virtual-ip-address ipaddr/mask-length

f. Activate the backup VR instance:
   enable

g. Inspect the configuration for the owner VR:
   show vrrp vlan vid vrid vrid-# config

   Leave the advertisement interval for backup routers at the default (1 second). For more
   on this topic, see “Changing VR advertisement interval and source IP address” (page 268).

3. Repeat step 2 for each backup router on the same VR.

Example configuration

In VR 1, below, R1 is the owner and the current master router, and R2 is the (only) backup in the
VR. If R1 becomes unavailable, VR 1 fails over to R2.

Figure 46 Example of a basic VRRP configuration

<table>
<thead>
<tr>
<th>VLAN 10 IP</th>
<th>VR 1 IP</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router 1</td>
<td>10.10.1</td>
<td>10.10.1</td>
</tr>
<tr>
<td>Router 2</td>
<td>10.10.23</td>
<td>10.10.1</td>
</tr>
</tbody>
</table>
Example 148 VRRP configuration for Router 1 (R1) in Figure 46 (page 291)

HP Switch(config)# router vrrp
HP Switch(config)# vlan 10
HP Switch(vlan-10)# vrrp vrid 1
HP Switch(vlan-10-vrid-1)# owner
HP Switch(vlan-10-vrid-1)# virtual-ip-address 10.10.10.1 255.255.255.0
HP Switch(vlan-10-vrid-1)# enable
HP Switch(vlan-10-vrid-1)# show vrrp vlan 10 vrid 1 config
VRRP Virtual Router Configuration Information
Vlan ID : 10
Virtual Router ID : 1

<table>
<thead>
<tr>
<th>Administrative Status [Disabled]</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode [Uninitialized]</td>
<td>owner</td>
</tr>
<tr>
<td>Priority [100]</td>
<td>255</td>
</tr>
<tr>
<td>Advertisement Interval [1]</td>
<td>1</td>
</tr>
<tr>
<td>Preempt Mode [True]</td>
<td>True</td>
</tr>
<tr>
<td>Primary IP Address : Lowest</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>10.10.10.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

This router is the owner for VR 1 in VLAN 10.

Because this router is the owner, the priority is fixed at 255 and cannot be changed.

For the same reason, the Preempt mode cannot be changed.

Because there is only one virtual IP address configured on the VR, the source address included with advertisements from this VR is the same as the virtual IP address for the VR.

Example 149 VRRP configuration for Router 2 (R2) in Figure 46 (page 291)

HP Switch(config)# router vrrp
HP Switch(config)# vlan 10
HP Switch(vlan-10)# vrrp vrid 1
HP Switch(vlan-10-vrid-1)# backup
HP Switch(vlan-10-vrid-1)# virtual-ip-address 10.10.10.1/24
HP Switch(vlan-10-vrid-1)# enable
HP Switch(vlan-10-vrid-1)# show vrrp vlan 10 vrid 1 config
VRRP Virtual Router Configuration Information
Vlan ID : 10
Virtual Router ID : 1

<table>
<thead>
<tr>
<th>Administrative Status [Disabled]</th>
<th>Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode [Uninitialized]</td>
<td>backup</td>
</tr>
<tr>
<td>Priority [100]</td>
<td>100</td>
</tr>
<tr>
<td>Advertisement Interval [1]</td>
<td>1</td>
</tr>
<tr>
<td>Preempt Mode [True]</td>
<td>True</td>
</tr>
<tr>
<td>Primary IP Address : Lowest</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td></td>
</tr>
<tr>
<td>Subnet Mask</td>
<td></td>
</tr>
<tr>
<td>10.10.10.1</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

This router is a backup in VR 1 for VLAN 10.

Because this router is a backup, the priority is set by default to 100 and can be changed to manipulate the precedence for backup routers in the VR.

On a backup router, the Preempt mode can be changed. However, in a VR having only one backup, Preempt mode has no effect.

Associating more than one VIP with a VR

If a VLAN is configured with more than 32 subnets and it is necessary to apply VRRP to all of these subnets, it is necessary to associate more than one VIP with a VR.

Because a VLAN on the routers supports up to 32 VRs, applying VRRP to a higher number of subnets in the VLAN requires multiple VIPs in one or more VRs.

If the owner of a VR is associated with multiple VIPs, the backup routers belonging to the same VR must also be associated with the same set of VIPs. If the VIPs on the owner are not also on the backups, a misconfiguration exists. VRRP advertisement packets sent by the VR master will be dropped by the VR backups because of a mismatch among VIPs.

Dynamically changing the priority of the VR

The dynamic priority change feature provides the ability to dynamically change the priority of the virtual router (VR) when certain events occur. The backup VR releases VIP control by reducing its
priority when tracked entities such as ports, trunks, or VLANs go down. You can also force the backup to take ownership of the VR if you have previously caused it to release control.

In normal VRRP operation, one router (Router-1) is in the master state and one router (Router-2) is in the backup state. Router-1 provides the default gateway for the host. If Router-1 goes down for any reason, the backup router, Router-2, provides the default gateway for the host.

Figure 47 Example VRRP configuration

If all the tracked entities configured on Router-1 go down, Router-1 begins sending advertisements with a priority of zero. This causes Router-2 to take control of the virtual IP.

Any applications or routing protocols, such as RIP or OSPF, on Router-1 that were using its IP address are no longer able to use that IP interface. Router-1 does not respond to any ARP requests for that IP address. Router-2 takes control of the IP address and responds to ARP requests for it with the virtual MAC address that corresponds to VRID-1.

NOTE: A backup VR switches to priority zero instead of its configured value when all of its tracked entities go down. An owner VR always uses priority 255 and never relinquishes control voluntarily.

Failover operation

Failover operation involves handing off the VR’s control of the virtual IP to another VR. Once a failover command is issued, the VR begins sending advertisements with priority zero instead of the configured priority. When the VR detects a peer VR taking control, it releases control of the virtual IP and ceases VR operation until a failback is executed. Failover occurs on only a backup VR operating as master.

If you specify the with-monitoring option, the VR continues to monitor the virtual IP after ceasing VR operation. If the master VR goes down, it then retakes control of the virtual IP.

Pinging the virtual IP of a backup router

When in compliance with RFC 3768, only owner VRs reply to ping requests (ICMP echo requests) to the VIP. When the virtual IP ping option is enabled, a backup VR operating as the master can respond to ping requests made to the VIP. This makes it possible to test the availability of the default gateway with ping. A non-owner VR that is not master drops all packets to the VIP.

NOTE: This feature is not a part of RFC 3768. Enabling this feature results in non-compliance with RFC 3768 rules.
Using the Pre-empt Delay Timer

To maintain availability of the default gateway router, the VRRP advertises a “virtual” router to the hosts. At least two other physical routers are configured to be virtual routers, but only one router provides the default router functionality at any given time. If the owner router or its VLAN goes down, the backup router takes over. When the owner router comes back on line (fail-back), it takes control of the VIP that has been assigned to it. It begins sending out VRRP advertisement packets at regular intervals. The backup router receives the VRRP advertisement packet and transitions to the backup state.

When OSPF is also enabled on the VRRP routers

When OSPF is enabled on the routers and a fail-back event occurs, the owner router immediately takes control of the VIP and provides the default gateway functionality. If OSPF has not converged, the route table in the owner router may not be completely populated. When the hosts send packets to the default gateway, the owner router may not know where to send them and packets may be dropped.

⚠️ CAUTION: While you can run OSPF and VRRP concurrently on a router, it is best not to run VRRP with other routing protocols, such as RIP or OSPF, on the same interface or VLAN, as this can create operational issues.

Configuring the PDT

The VRRP PDT allows you to configure a period of time before the VR takes control of the VIP. It does not transition to the master state until the timer period expires. The timer value configured should be long enough to allow OSPF convergence following OSPF updates.

The PDT is applied only during initialization of the router, that is, when the router is rebooting with the VRRP parameters present in the startup config file.

VRRP preempt mode with LACP and older HP devices

There can be an issue with VRRP preempt mode if an older HP device (2524, 2650, 2848, 3400, or 5300) is the intermediate device connecting to a VRRP router and has LACP set in "enable, passive" mode. This mode is set by default on older HP devices, whereas it is disabled by default on later models such as the HP Series 5400zl. HP recommends that you use compatible LACP settings on devices that connect with VRRP routers on VRRP VLANs.

What occurs at startup

When the owner router comes online, it waits for the configured amount of time before taking control of the VIP. This period of time is calculated as follows:

If the value of the master down time (3 * advertisement interval) is less than or equal to the preempt delay time, the owner router will wait until the master down time (3 * advertisement interval) has expired.

During this waiting period, if the owner router receives a VRRP packet for its VIP from the backup router, it waits until the PDT expires before taking control of its VIP. If the owner router does not receive any VRRP packets and the master down time expires, the owner router can take control of its VIP immediately.

If the value of the master down time (3 * advertisement interval) is greater than the preempt delay time, the owner router will wait until the PDT expires before taking control of its VIP.
Selecting a value for the PDT

You should select the value for the PDT carefully to allow time for OSPF to populate the owner router’s route tables. The choice depends on the following:

- The OFPF router dead interval—the number of seconds the OSPF router waits to receive a hello packet before assuming its neighbor is down.
- The number of router interfaces that participate in OSPF
- The time it may take from reception of the OSPF packets to when the population of the route table is completed.

There are trade-offs between selecting a small advertisement value and a large PDT. A small advertisement value results in a faster failover to the backup router. A larger PDT value allows OSPF to converge before the owner router takes back control of its VIP.

Choosing a large PDT value (greater than the master down time) may result in an unnecessary failover to the backup router when the VRRP routers (owner and backup) start up together. Choosing a large advertisement interval and thereby a large master down time results in a slower failover to the backup router when the owner router fails.

Possible configuration scenarios

PDT=zero seconds

This is the default behavior. It works in the same way that VRRP works currently.

PDT is greater than or equal to the master down time (3 times the advertisement interval)

a. An owner VR after reboot—waits for the master down time. If the owner router does not receive a packet during this time, it becomes the master. If it receives a VRRP advertisement from its peer during this time, it waits until the expiration of the preempt delay time before becoming the master.

b. A backup VR after reboot—waits for the master down time. If the backup router does not receive a packet during this time, it becomes the master. If it receives a VRRP advertisement from its peer during this time, and it has a higher priority value than this peer, it waits until the expiration of the preempt delay time before becoming the backup.

PDT is less than the master down time

a. Owner router—becomes the master after expiration of the PDT.

b. Backup router—becomes the backup after expiration of the PDT if it does not receive a VRRP advertisement from a higher priority peer (or the owner).

When the PDT is not applicable

Once the router has rebooted and is in steady state VRRP operation, the PDT is not applicable if:

- The VRRP VLAN goes down and comes back up.
- The VR is disabled and re-enabled.
- VRRP is globally disabled and then re-enabled.

Backward compatibility

If a VRRP router functions with an older version that does not have the PDT feature, it will take over VIP control immediately on startup or when there is a fail-back event. There should be no backward compatibility issues.
Error messages

<table>
<thead>
<tr>
<th>Error</th>
<th>Error message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempting to assign the PDT to the VR before declaring it as an owner or backup</td>
<td>The Virtual Router must be defined as an owner or backup router first.</td>
</tr>
<tr>
<td>Attempting to assign an out of range PDT to the VR instance</td>
<td>Invalid input: out of range value</td>
</tr>
<tr>
<td>Attempting to change the PDT value when the VR is active</td>
<td>VR operation must be &quot;down&quot; prior to modifying VR’s parameters</td>
</tr>
</tbody>
</table>

Standards compliance

VRRP on the switches includes the following:

- Complies with RFC 3768 VRRP, except for maximum number of VRs per VLAN, which is 32 on the routers.
- Compatible with HP Series 9300m routers, the HP 9408sl router, and the HP Series 8100fl switches. (VRRP on these devices is based on RFC 2338.)
- Complies with RFC 2787—Definitions of Managed Objects for VRRP, except for support for authentication-related values.
- Applies to use on IPv4 routers.

Operating notes

- VRRP advertisements not reaching the backup(s)
  If a master is forwarding traffic properly, but its backups are prevented from receiving the master’s VRRP advertisements, both routers will operate in the master mode for the VR. If this occurs, traffic for the applicable gateway will continuously alternate between routers (sometimes termed "flapping").
- Deleting an IP address used to support a VR
  See “General operating rules” (page 288).
- VR limits
  A VLAN allows up to 32 VRs, and a VR allows up to 32 IP addresses. This means that one VR can support up to 32 subnets. This capacity enables use of VRRP on all subnets in a VLAN that has more than 32 subnets.
- IPv4
  The routers support IPv4 IP addressing for VRRP applications.
- Authentication type
  As per
  RFC 3768, the authentication type for VRRP packets inbound on the router is 0 (zero; that is, "no authentication"). Packets with other authentication types are dropped, and authentication type is not supported in the VRRP MIB. If you are coordinating the use of VRRP on the routers
with another vendor’s implementation based on an older RFC, you must set the authentication type to 0 (zero) on the other vendor’s device.

- **Proxy-ARP requests and MAC addresses**
  The following table shows which MAC address is returned in response to a proxy-ARP request.

<table>
<thead>
<tr>
<th>Configured as:</th>
<th>Administratively:</th>
<th>Returns:</th>
</tr>
</thead>
<tbody>
<tr>
<td>owner</td>
<td>Enabled</td>
<td>VRRP MAC address</td>
</tr>
<tr>
<td>owner</td>
<td>Disabled</td>
<td>Default VLAN MAC address</td>
</tr>
<tr>
<td>backup</td>
<td>Enabled, in master state</td>
<td>VRRP MAC address</td>
</tr>
<tr>
<td>backup</td>
<td>Enabled, not in master state</td>
<td>VRRP router does not respond to proxy-ARP request.</td>
</tr>
<tr>
<td>backup</td>
<td>Disabled</td>
<td>Default VLAN MAC address</td>
</tr>
</tbody>
</table>

**Dynamic priority change operating notes**

- There are no backward compatibility issues with the VRRP dynamic priority change feature. If a VRRP router has an older firmware version that does not have the dynamic priority change feature, it will not have the needed configuration options.
- The VR’s operating VLAN cannot be configured as a tracking VLAN for that VR.
- Ports that are part of a trunk cannot be tracked.
- A port that is tracked cannot be included in a trunk.
- Trunks that are tracked cannot be removed; you are not able to remove the last port from the trunk.
- LACP (active or passive) cannot be enabled on a port that is being tracked.
- If a VLAN is removed or a port becomes unavailable, the configuration is retained and they are tracked when they become available again.
- After the owner VR relinquishes control of its IP address, that IP address becomes unavailable to all other applications and routing protocols such as RIP and OSPF.
- To avoid operational issues, HP recommends that VRRP is not run on the same interface/VLAN with other routing protocols, such as RIP and OSPF.

**Event Log messages**

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure to send out pkt for vrid vrid-# , vid vid-#</td>
<td>A VRRP packet could not be sent out for the indicated VR on the specific VLAN because of any system-dependent problem. If packets could not be sent out, the expected protocol operation may be hampered.</td>
</tr>
<tr>
<td>No VR with vrid vrid-# found on vid vid-#</td>
<td>Indicates a VRRP packet received for a VR that does not exist on the VLAN. This can indicate asymmetric configuration of VRs across VRRP routers.</td>
</tr>
<tr>
<td>Pkt recd on a non-VRRP Vlan with vid vid-#</td>
<td>A VRRP packet was received on a VLAN that does not have any VRs. This could possibly be a result of misconfiguration of VRs on VLANs.</td>
</tr>
<tr>
<td>Pkt recd with version number ver-# , expected ver-#</td>
<td>A VRRP packet was received with a wrong version number.</td>
</tr>
<tr>
<td>Message</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>Vrid vrid-# on Vid vid-# has taken backup IP ctrl</td>
<td>The owner of a VR is not available and a backup has taken master control of the VR.</td>
</tr>
<tr>
<td>Vrid vrid-# on Vid vid-# has taken owner IP ctrl</td>
<td>The owner of a VR has taken master control of the VR, either following a reboot or a failback from a backup serving as master.</td>
</tr>
<tr>
<td>Vrid vrid-# on Vid vid-# lost backup IP ctrl</td>
<td>The indicated VR has been preempted by either the owner or a higher-priority master.</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# IP addr is duplicated on the network</td>
<td>The VIP owned by the indicated VR on the indicated VLAN is duplicated on the network.</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# recd pkt from a duplicate master</td>
<td>A VRRP packet was received from a duplicate master VR by the indicated VR on the indicated VLAN.</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# recd pkt with advt int mismatch</td>
<td>The indicated VR on the indicated VLAN has received a VRRP master message carrying a different advertisement interval than is configured on the receiving VR and has dropped the packet.</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# recd pkt with auth type mismatch</td>
<td>Indicates the VR has received a packet with the authentication type set to 1 or 2. These are generally valid authentication types, but are not required by RFC 3768. Thus, the software supports only an authentication type of 0 (zero), and VRRP packets with 1 or 2 for authentication type are dropped. See &quot;Authentication type&quot; under “Operating notes” (page 296).</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# recd pkt with bad IP-TTL</td>
<td>A VRRP packet was received by the indicated VR on the indicated VLAN with an IP TTL value not equal to 255.</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# recd pkt with checksum error</td>
<td>The indicated VR on the indicated VLAN has received a VRRP advertisement packet with a checksum error. The VR has therefore dropped that packet.</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# recd pkt with invalid auth type</td>
<td>Indicates the VR has received a VRRP packet with an authentication type set to a value other than the 0, 1, or 2 (allowed by RFC 3768) and has dropped the packet.</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# recd pkt with IP address mismatch</td>
<td>A VRRP packet was received by the indicated VR on the indicated VLAN with VIPs that did not match the VIPs configured on the receiver VR.</td>
</tr>
<tr>
<td>Vrid vrid-, Vid vid-# recd pkt with invalid type</td>
<td>A VRRP packet was received by the indicated VR on the indicated VLAN with the packet type not equal to 1.</td>
</tr>
<tr>
<td>VRRP has been disabled on this router</td>
<td>VRRP was disabled at the global config level.</td>
</tr>
<tr>
<td>VRRP has been enabled on this router</td>
<td>VRRP was enabled at the global config level.</td>
</tr>
</tbody>
</table>

### Error messages—Track interface

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VR must be defined as &quot;backup&quot; first</td>
<td>You have to declare a VR as backup before assigning a track interface to it.</td>
</tr>
<tr>
<td>Invalid input: out of range value</td>
<td>You have to assign a valid port or trunk to the VR instance.</td>
</tr>
<tr>
<td>VR operation must be &quot;down&quot; prior to modifying VR’s parameters</td>
<td>You cannot change the track interface when the VR is active. Use the no enable command to disable the VR.</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Can’t track a port that is part of a trunk</td>
<td>You cannot configure tracking on a port that is a member of a trunk.</td>
</tr>
<tr>
<td>Tracking is disabled on owner</td>
<td>You cannot configure a track interface on an owner VR.</td>
</tr>
<tr>
<td>Cannot remove trunk being tracked by VRRP</td>
<td>You cannot remove a trunk that is being tracked by a VR.</td>
</tr>
<tr>
<td>Cannot enable LACP on a VRRP tracked port</td>
<td>You cannot enable LACP on a port that is being tracked by a VR.</td>
</tr>
<tr>
<td>Too many entities to track</td>
<td>You have selected too many entities to be tracked by the VR.</td>
</tr>
<tr>
<td>Cannot track trunk/LACP member</td>
<td>You cannot track the specified trunk or LACP member.</td>
</tr>
<tr>
<td>VRRP tracked port is not allowed in trunk</td>
<td>You cannot add this tracked port to a trunk.</td>
</tr>
<tr>
<td>VRRP tracked port is not allowed in LACP</td>
<td>You cannot use LACP with the tracked port.</td>
</tr>
<tr>
<td>Operation is not permitted on VR when it is configured as owner or is uninitialized.</td>
<td>The VR must be a backup and initialized in order to execute the operation.</td>
</tr>
</tbody>
</table>
13 Border Gateway Protocol (BGP)

Global BGP configuration

Table 42 Global BGP configuration commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>router bgp as-# no router bgp</td>
<td>Configures a BGP routing process.</td>
<td>Not enabled.</td>
<td>(page 300)</td>
<td></td>
</tr>
<tr>
<td>bgp router-id router-id no bgp router id</td>
<td>Configures a fixed router ID for the local Border Gateway Protocol (BGP) routing process.</td>
<td></td>
<td>(page 300)</td>
<td></td>
</tr>
<tr>
<td>[no] network ipv4/mask [route-map route-map-name]</td>
<td>To specify the networks to be advertised by the Border Gateway Protocol (BGP) routing processes, use the network command.</td>
<td></td>
<td>(page 301)</td>
<td></td>
</tr>
<tr>
<td>[no] bgp timers keep-alive hold-time</td>
<td>To adjust BGP network timers, use the bgp timers command in router configuration mode.</td>
<td></td>
<td>(page 301)</td>
<td></td>
</tr>
<tr>
<td>[no] enable disable</td>
<td>Re-enables the state contained within this node and all child nodes of the Border Gateway Protocol (BGP) process.</td>
<td>Disabled</td>
<td>(page 301)</td>
<td></td>
</tr>
</tbody>
</table>

Configuring a BGP routing process

Syntax:

```
router bgp as-
no router bgp
```

Configures a BGP routing process. To remove the routing process, use the no form of the command. This command is used in the configuration context only. This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Configuring a fixed router ID for local BGP routing process

Syntax:

```
bgp router-id router-id
no bgp router id
```

Configures a fixed router ID for the local Border Gateway Protocol (BGP) routing process. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the no form of this command.
The `bgp router-id` command is used to configure a fixed router ID for a local BGP routing process. The router ID is entered in the IP address format. Any valid IP address can be used.

### Specifying the networks to be advertised by BGP routing process

**Syntax:**

```
[no] network ipv4/mask [route-map route-map-name]
```

To specify the networks to be advertised by the Border Gateway Protocol (BGP) routing processes, use the `network` command. To remove an entry from the routing table, use the `no` form of this command.

BGP networks can be learned from connected routes, from dynamic routing, and from static route sources. The maximum number of network commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

### Adjusting BGP network timers

**Syntax:**

```
[no] bgp timers keep-alive hold-time
```

To adjust BGP network timers, use the `bgp timers` command in router configuration mode. To reset the BGP timing defaults, use the `no` form of this command.

### Re-enabling state contained within nodes of BGP processes

**Syntax:**

```
[no] enable disable
```

Re-enables the state contained within this node and all child nodes of the Border Gateway Protocol (BGP) process. The `disable` command disables the state contained within this node and all child nodes. The default is for the state to be disabled.

### Global BGP policy configuration

**Table 43 Global BGP policy configuration commands**

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[no] bgp open-on-accept</code></td>
<td>Delays sending the BGP Open message until an OPEN message is received.</td>
<td></td>
<td>(page 303)</td>
<td></td>
</tr>
<tr>
<td><code>[no] bgp maximum-prefix max-routes</code></td>
<td>Specifies the maximum number of routes that BGP will accept for installation into RIB.</td>
<td></td>
<td>(page 303)</td>
<td></td>
</tr>
<tr>
<td><code>[no] bgp always-compare-med</code></td>
<td>Enables the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.</td>
<td></td>
<td>(page 303)</td>
<td></td>
</tr>
<tr>
<td>Command syntax</td>
<td>Description</td>
<td>Default</td>
<td>CLI reference</td>
<td>Menu reference</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>[no] bgp allowas-in num-loops</td>
<td>Specifies the number of time an Autonomous System number can appear in the AS_PATH.</td>
<td></td>
<td>(page 303)</td>
<td></td>
</tr>
<tr>
<td>[no] bgp bestpath as-path-ignore</td>
<td>Configures Border Gateway Protocol (BGP) to not consider the autonomous system (AS)-path during best path route selection.</td>
<td></td>
<td>(page 304)</td>
<td></td>
</tr>
<tr>
<td>[no] bgp bestpath compare-originator-id</td>
<td>Specifies to break ties between routes based the Originator ID value instead of the neighbor’s router ID.</td>
<td></td>
<td>(page 304)</td>
<td></td>
</tr>
<tr>
<td>[no] bgp bestpath compare-router-id</td>
<td>To configure a Border Gateway Protocol (BGP) routing process to compare identical routes received from different external peers during the best path selection process and to select the route with the lowest router ID as the best path, use the bgp bestpath compare-router-id command in router configuration mode.</td>
<td></td>
<td>(page 304)</td>
<td></td>
</tr>
<tr>
<td>[no] bgp bestpath med-missing-as-worst</td>
<td>To configure a Border Gateway Protocol (BGP) routing process to assign a value of infinity (max possible) to routes that are missing the Multi Exit Discriminator (MED) attribute (making the path without a MED value the least desirable path), use the bgp bestpath med missing-as-worst command in router configuration mode.</td>
<td></td>
<td>(page 304)</td>
<td></td>
</tr>
<tr>
<td>[no] bgp default-metric med-out</td>
<td>Causes a BGP MED to be set on routes when they are advertised to peers.</td>
<td></td>
<td>(page 304)</td>
<td></td>
</tr>
<tr>
<td>[no] distance bgp ext-dist int-dist loc-dist</td>
<td>A route’s preference specifies how active routes that are learned from BGP (compared</td>
<td></td>
<td>(page 305)</td>
<td></td>
</tr>
</tbody>
</table>
### Delaying sending the BGP open message

**Syntax:**

```plaintext
[no] bgp open-on-accept
```

Delays sending the BGP Open message until an OPEN message is received. When this command is specified, an OPEN message will be immediately sent when the TCP connection has completed for configured peers. If the peer is not configured (is matched by an allow clause, but not a peer command), it will continue to wait for the OPEN message from the remote peer before sending its own BGP OPEN message.

### Maximum routes that BGP will accept for installation into RIB

**Syntax:**

```plaintext
[no] bgp maximum-prefix max-routes
```

Specifies the maximum number of routes that BGP will accept for installation into RIB. Use the no form of the command to set the parameter to its default value.

### Enabling comparison of MED for paths from neighbors in different autonomous systems

**Syntax:**

```plaintext
[no] bgp always-compare-med
```

Enables the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. To disallow the comparison, use the no form of this command.

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. During the best-path selection process, MED comparison is done only among paths from the same autonomous system. The `bgp always-compare-med` command is used to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

### Specifying number of times an AS number can appear in AS_PATH

**Syntax:**

```plaintext
[no] bgp allowas-in num-loops
```
Specifies the number of times an Autonomous System number can appear in the AS_PATH. Use the no form of the command to set the parameter to its default value of ‘1’.

Configuring BGP to not consider AS_PATH

Syntax:

```plaintext
[no] bgp bestpath as-path-ignore
```

Configures Border Gateway Protocol (BGP) to not consider the autonomous system (AS)-path during best path route selection. To restore default behavior and configure BGP to consider the AS-path during route selection, use the no form of this command. By default, the AS-path is considered during BGP best path selection.

Breaking ties between routes based on originator ID value

Syntax:

```plaintext
[no] bgp bestpath compare-originator-id
```

Specifies to break ties between routes based on the Originator ID value instead of the neighbor’s router ID. Use the no form of the command to not compare routes based on originator ID.

Comparing identical routes received from different external peers

Syntax:

```plaintext
[no] bgp bestpath compare-router-id
```

To configure a Border Gateway Protocol (BGP) routing process to compare identical routes received from different external peers during the best path selection process and to select the route with the lowest router ID as the best path, use the `bgp bestpath compare-router-id` command in router configuration mode. To return the BGP routing process to the default operation, use the no form of this command.

The behavior of this command is disabled by default; BGP selects the route that was received first when two routes with identical attributes are received.

Assigning value of infinity to routes missing MED attribute

Syntax:

```plaintext
[no] bgp bestpath med-missing-as-worst
```

To configure a Border Gateway Protocol (BGP) routing process to assign a value of infinity (max possible) to routes that are missing the Multi Exit Discriminator (MED) attribute (making the path without a MED value the least desirable path), use the `bgp bestpath med missing-as-worst` command in router configuration mode. To return the router to the default behavior (assign a value of 0 to the missing MED), use the no form of this command.

Setting BGP MED on routes when advertised to peers

Syntax:

```plaintext
[no] bgp default-metric med-out
```

Causes a BGP MED to be set on routes when they are advertised to peers. This value applies to all BGP peers. It can be overridden on a per-peer basis. The no form of this command, `no default-metric`, removes the configured value.
Specifying a route's preference

**Syntax:**

```
[no] distance bgp ext-dist int-dist loc-dist
```

A route’s preference specifies how active routes that are learned from BGP (compared to other protocols) will be selected. When a route has been learned from more than one protocol, the active route will be selected from the protocol with the lowest preference. Each protocol has a default preference in this selection. This preference can be overridden by a preference value specified on the peer.

Enabling client-to-client route reflection

**Syntax:**

```
[no] bgp client-to-client-reflection
```

Enables or disables client-to-client route reflection. When acting as a route-reflector, this functionality is enabled by default.

Specifying cluster ID when BGP router is route-reflector

**Syntax:**

```
[no] bgp cluster-id ip-address
```

Specifies the cluster ID to be used when the BGP router is used as a route-reflector. The cluster ID default is the router ID.

BGP graceful restart

**Table 44 Graceful restart commands**

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp graceful-restart { restart-time val</td>
<td>[stalepath-time val]}</td>
<td>Configures BGP graceful restart timers.</td>
<td>(page 306)</td>
<td></td>
</tr>
<tr>
<td>[no] bgp log-neighbor-changes [prefix-list prefix-list-name]</td>
<td>Enables or disables BGP event logging.</td>
<td>(page 306)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr description desc</td>
<td>Describes a neighbor.</td>
<td>(page 306)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] nonstop</td>
<td>Configured under BGP routing context, enables nonstop forwarding for BGP on the 8200 series devices and enables the router to retain the ip forwarding table across redundancy switchover.</td>
<td>(page 306)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring BGP graceful restart timers

**Syntax:**

```
bgp graceful-restart { restart-time val | [stalepath-time val]}
```

Configures BGP graceful restart timers as follows:

- **restart-time**
  The time in seconds to wait for a graceful restart capable neighbor to re-establish BGP peering.

- **stalepath-time**
  The time in seconds to hold stale routes for a restarting peer.

Enabling event logging

**Syntax:**

```
[no] bgp log-neighbor-changes [prefix-list prefix-list-name]
```

Enables or disables BGP event logging. Optionally, specify a prefix-list to filter log messages from specific BGP neighbors only.

Describing a neighbor

**Syntax:**

```
[no] neighbor ipv4-addr description desc
```

Describes a neighbor.

Enabling nonstop forwarding for BGP

**Syntax:**

```
[no] nonstop
```

Configured under BGP routing context, enables nonstop forwarding for BGP on the 8200 series devices and enables the router to retain the ip forwarding table across redundancy switchover.

Neighbor configuration and neighbor policy configuration

### Table 45 Neighbor configuration and neighbor policy configuration commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor ipv4-addr remote-as as-# no neighbor ipv4-addr</td>
<td>Adds an entry to the BGP neighbor table in router configuration mode.</td>
<td>(page 309)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr graceful-restart</td>
<td>Exports the graceful restart capabilities to a peering session for the ipv4 unicast address family. This feature is available only on the 8200 series devices.</td>
<td>(page 309)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 45 Neighbor configuration and neighbor policy configuration commands (continued)

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] neighbor ipv4-addr dynamic</td>
<td>Specifies whether to enable or disable dynamic capabilities.</td>
<td></td>
<td>(page 309)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr updated-source ipv4-addr</td>
<td>Specifies the IP address to be used on the local end of the TCP connection with the peer.</td>
<td></td>
<td>(page 309)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr allows-in num-loops</td>
<td>Specifies the number of times this autonomous system can appear in an AS path.</td>
<td>When not configured, or when using the no version of the command, the value of as-loops is set to its default value of 1.</td>
<td>(page 310)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr as-override</td>
<td>Causes all occurrences of our peer’s AS to be replaced with one from an export.</td>
<td></td>
<td>(page 310)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr ignore-leading-as</td>
<td>Some routers are capable of propagating routes without appending their own autonomous system number to the AS Path.</td>
<td>By default, BGP will drop such routes.</td>
<td>(page 310)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr local-as as-#</td>
<td>Identifies the autonomous system (AS) that BGP is representing to a peer.</td>
<td>The default AS number for this command is the current AS (configured with the router bgp command in Global Configuration mode).</td>
<td>(page 310)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr maximum-prefix max-routes</td>
<td>Specifies the maximum number of routes that BGP will accept for installation into RIB.</td>
<td>The value defaults to “unlimited” if not specified, or if using the no version of the command.</td>
<td>(page 310)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr out-delay sec</td>
<td>The specified integer represents the amount of time a route must be present in the routing database before it is exported into BGP</td>
<td>Defaults to 0 if no specified or if un-configured by using no version of command.</td>
<td>(page 310)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr weight weight</td>
<td>Preferences are the first criteria of comparison for route selection.</td>
<td>This value defaults to the globally configured preference if it is not specified.</td>
<td>(page 305)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr send-community</td>
<td>To specify that a community’s attribute should be sent to a BGP neighbor, use the neighbor send-community command in address</td>
<td></td>
<td>(page 311)</td>
<td></td>
</tr>
<tr>
<td>Command syntax</td>
<td>Description</td>
<td>Default</td>
<td>CLI reference</td>
<td>Menu reference</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>Processes sending of MEDs and for handling received MEDs.</td>
<td></td>
<td>(page 311)</td>
<td></td>
</tr>
<tr>
<td>use-med</td>
<td></td>
<td>By default MEDs are used to choose which route to use.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>To set the timers for a specific BGP peer, use the neighbor keep-alive command in router configuration mode.</td>
<td></td>
<td>(page 311)</td>
<td></td>
</tr>
<tr>
<td>timers keep-alive hold-time</td>
<td>The values of keep-alive and hold-time default to 60 and 180 seconds, respectively.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>clear ip bgp [neighbor ipv4-addr] [soft ]</td>
<td>Resets BGP peering sessions, sends route refresh requests if ‘soft’.</td>
<td></td>
<td>(page 311)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>Enables or disables multi-hop peering with the specified EBGP peer, and optionally indicates the maximum number of hops (TTL).</td>
<td></td>
<td>(page 311)</td>
<td></td>
</tr>
<tr>
<td>ibgp-multihop [ttl]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>Forces BGP to use the router’s outbound interface address as the next hop for the route updates to the peer.</td>
<td></td>
<td>(page 312)</td>
<td></td>
</tr>
<tr>
<td>next-hop-self</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>If enabled, does not initiate a peering connection to the peer.</td>
<td></td>
<td>(page 312)</td>
<td></td>
</tr>
<tr>
<td>passive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>Specifies whether the private AS # should be removed from the as-path attribute of updates to the EBGP peer.</td>
<td></td>
<td>(page 312)</td>
<td></td>
</tr>
<tr>
<td>remove-private-as</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>Acts as a route-reflector for the peer.</td>
<td></td>
<td>(page 312)</td>
<td></td>
</tr>
<tr>
<td>route-reflector-client</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>Shuts down the BGP peering session without removing the associated peer configuration.</td>
<td></td>
<td>(page 312)</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr</td>
<td>Enables or disables the advertisement of route-refresh capability in the Open message sent to the peer.</td>
<td></td>
<td>(page 312)</td>
<td></td>
</tr>
<tr>
<td>route-refresh</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Adding entry to BGP neighbor table in router configuration mode

**Syntax:**

neighbor ipv4-addr remote-as as-#
no neighbor ipv4-addr

Adds an entry to the BGP neighbor table in router configuration mode. To remove an entry from the table, use the no form of this command.

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the router bgp global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

Exporting graceful restart capabilities to peering session

**Syntax:**

[no] neighbor ipv4-addr graceful-restart

Exports the graceful restart capabilities to a peering session for the ipv4 unicast address family. Note that this feature is available only on the 8200 series devices.

Enabling or disabling dynamic capabilities

**Syntax:**

[no] neighbor ipv4-addr dynamic

Specifies whether to enable or disable dynamic capabilities.

BGP Dynamic Capabilities allow the communication of a change in a BGP peer’s capabilities without having to restart the peering session. The BGP implementation is done on a per-peer basis and in such a way that dynamic capabilities are supported as long as the BGP peer supports BGP Dynamic Capabilities. BGP advertises Dynamic Capabilities in the OPEN message. If a BGP peer advertises support for BGP Dynamic Capabilities in the OPEN message, then it turns on Dynamic Capabilities. Otherwise, the dynamic capabilities for this peer will be disabled. BGP supports the following BGP Dynamic Capabilities:

- Graceful restart
- Route refresh

Specifying IP address for local end of TCP connection with peer

**Syntax:**

[no] neighbor ipv4-addr updated-source ipv4-addr

Specifies the IP address to be used on the local end of the TCP connection with the peer. This is the address of a broadcast, NBMA or loopback interface and the local address of a point-to-point interface. For external peers, the local address must be on an interface that is shared with the peer or with the peer’s gateway when a gateway is used. A session with an external peer will be opened only when an interface with the appropriate local address (through which the peer or gateway address is directly reachable) is operating. For internal peers, a peer session will be maintained when any interface with the specified local address is operating. In any case, an incoming connection will be recognized as a match for a configured peer only if it is addressed to the configured local address.
Specifying times autonomous system can appear in an AS path

Syntax:

```
[no] neighbor ipv4-addr allowas-in num-loops
```

Specifies the number of times this autonomous system can appear in an AS path. When not configured, or when using the no version of the command, the value of as-loops is set to its default value of 1.

Replacing occurrences of peer's AS with one from export

Syntax:

```
[no] neighbor ipv4-addr as-override
```

Causes all occurrences of our peer’s AS to be replaced with one from an export.

Allowing BGP to keep routes without AS number

Syntax:

```
[no] neighbor ipv4-addr ignore-leading-as
```

Some routers are capable of propagating routes without appending their own autonomous system number to the AS Path. By default, BGP will drop such routes. Turning this parameter “on” allows BGP to keep these routes. This option should be used only if there is no doubt that these peers are not normal routers.

Identifying AS that BGP is representing to peer

Syntax:

```
[no] neighbor ipv4-addr local-as as-
```

Identifies the autonomous system (AS) that BGP is representing to a peer. The default AS number for this command is the current AS (configured with the `router bgp` command in Global Configuration mode). This command is valid only for external peers.

Specifying maximum number of routes for installation into RIB

Syntax:

```
[no] neighbor ipv4-addr maximum-prefix max-routes
```

Specifies the maximum number of routes that BGP will accept for installation into RIB. The value defaults to “unlimited” if not specified, or if using the no version of the command.

Time route is present in database before exported to BGP

Syntax:

```
[no] neighbor ipv4-addr out-delay sec
```

The specified integer represents the amount of time a route must be present in the routing database before it is exported into BGP. Defaults to 0 if no specified or if unconfigured by using no version of command.
Comparison for route selection

Syntax:

\[\text{[no]} \text{neighbor ipv4-addr weight weight}\]

Preferences are the first criteria of comparison for route selection. This value defaults to the globally configured preference if it is not specified.

Sending community's attribute to BGP neighbor

Syntax:

\[\text{[no]} \text{neighbor ipv4-addr send-community}\]

To specify that a community’s attribute should be sent to a BGP neighbor, use the neighbor send-community command in address family or router configuration mode. To remove the entry, use the no form of this command. By default the communities attribute is sent to all peers.

Processing sent and received MEDs

Syntax:

\[\text{[no]} \text{neighbor ipv4-addr use-med}\]

Processes sending of MEDS and for handling received MEDs. When two routes to the same destination are received from different peers within the same peers as, they could have different MEDs. When choosing between these routes, assuming that nothing else makes one preferable to the other (such as configured policy), the values of the differing MEDs are used to choose which route to use. In this comparison, the route with the lowest MED is preferred. Routes without MEDs are treated as having a MED value of zero. By default, MEDs are used to choose which route to use.

Setting timer for BGP peer

Syntax:

\[\text{[no]} \text{neighbor ipv4-addr timers keep-alive hold-time}\]

To set the timers for a specific BGP peer, use the neighbor timers command in router configuration mode. To clear the timers for a specific BGP peer, use the no form of this command. The values of keep-alive and hold-time default to 60 and 180 seconds, respectively.

The timers configured for a specific neighbor override the timers configured for all BGP neighbors using the timers command.

Resetting BGP peering session

Syntax:

\text{clear ip bgp [neighbor ipv4-addr][ soft ]}\n
Resets BGP peering sessions, sends route refresh requests if ‘soft’.

Enabling or disabling multi-hop peering

Syntax:

\[\text{[no]} \text{neighbor ipv4-addr ibgp-multihop [ttl]}\]

Enables or disables multi-hop peering with the specified EBGP peer, and optionally indicates the maximum number of hops (TTL).
Using router’s outbound interface address as next hop

Syntax:

\[ \text{[no]} \text{ neighbor ipv4-addr next-hop-self} \]
Forces BGP to use the router’s outbound interface address as the next hop for the route updates to the peer.

Specifying no peering connection to peer

Syntax:

\[ \text{[no]} \text{ neighbor ipv4-addr passive} \]
If enabled, does not initiate a peering connection to the peer.

Removing private AS number from updates to EBGP peer

Syntax:

\[ \text{[no]} \text{ neighbor ipv4-addr remove-private-as} \]
Specifies whether the private AS # should be removed from the as-path attribute of updates to the EBGP peer.

Acting as route-reflector for peer

Syntax:

\[ \text{[no]} \text{ neighbor ipv4-addr route-reflector-client} \]
Acts as a route-reflector for the peer.

Shutting down BGP peering session without removing peer configuration

Syntax:

\[ \text{[no]} \text{ neighbor ipv4-addr shutdown} \]
Shuts down the BGP peering session without removing the associated peer configuration.

Enabling or disabling advertisement of route-refresh capability in open message

Syntax:

\[ \text{[no]} \text{ neighbor ipv4-addr route-refresh} \]
Enables or disables the advertisement of route-refresh capability in the Open message sent to the peer.
BGP-IGP synchronization

### Table 46 BGP-IGP synchronization commands

<table>
<thead>
<tr>
<th>Command syntax</th>
<th>Description</th>
<th>Default</th>
<th>CLI reference</th>
<th>Menu reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>[no] redistribute protocol [route-map route-map-name]</td>
<td>Specifies routes to export into BGP. This command causes routes from the specified protocol to be considered for redistribution into BGP.</td>
<td>(page 313)</td>
<td>(page 313)</td>
<td></td>
</tr>
<tr>
<td>[no] neighbor ipv4-addr route-map route-map-name [[in]</td>
<td>[out]]</td>
<td>Route maps control the redistribution of routes between protocols.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Specifying routes to export into BGP

**Syntax:**

[no] redistribute protocol [route-map route-map-name]

Specifies routes to export into BGP. This command causes routes from the specified protocol to be considered for redistribution into BGP. Additionally, if a route map is specified, then routes from the specified protocol that match the named route map will be considered for redistribution into the current protocol. If the referenced route map has not yet been configured, then an empty route map is created with the specified name.

### Specifying route map to be exported in or out of BGP

**Syntax:**

[no] neighbor ipv4-addr route-map route-map-name[[in] | [out]]

Route maps control the redistribution of routes between protocols. Only after configuring a route map, can it then be specified in BGP. Use this command to specify a configured route map to be exported into or out of BGP. When the in version of this command is configured, all IPv4 announcements received from the specified neighbor should be run against the policy specified in the named route-map. When the out version of this command is used, it specifies that all IPv4 announcements sent to the specified neighbor should be run against the policy specified in the named route-map. After evaluating this policy, each route will be compared to the specified route-target export, to see if announcement is acceptable.

### Introduction

This chapter covers BGPv4 (RFC 4271), which is the defacto internet exterior gateway protocol used between ISPs.

The characteristics of BGP are as follows:

- Focusing on the control of route propagation and the selection of optimal routes rather than the route discovery and calculation, which makes BGP, an exterior gateway protocol different from interior gateway protocols such as OSPF and RIP.
- Using TCP to enhance reliability.
- Supporting CIDR.
• Reducing bandwidth consumption by advertising only incremental updates and therefore applicable to advertising a great amount of routing information on the Internet.
• Eliminating routing loops completely by adding AS path information to BGP routes.
• Providing abundant policies to implement flexible route filtering and selection.
• Good scalability.

A router advertising BGP messages is called a BGP speaker. It establishes peer relationships with other BGP speakers to exchange routing information. When a BGP speaker receives a new route or a route better than the current one from another AS, it will advertise the route to all the other BGP peers in the local AS.

BGP can be configured to run on a router in the following two modes:
• iBGP (internal BGP)
• eBGP (external BGP)

When a BGP speaker peers with another BGP speaker which resides in the same autonomous system, the session is referred to as an iBGP session and when a BGP speaker peers with a BGP speaker which resides in another autonomous system then the session is referred to as an eBGP session.

**BGP path attributes**

**Classification of path attributes**

Path attributes fall into four categories:

Well-known mandatory
• Must be recognized by all BGP routers and must be included in every update message. Routing information errors occur without this attribute.

Well-known discretionary
• Can be recognized by all BGP routers and optional to be included in every update message as needed.

Optional transitive
• Transitive attribute between ASs. A BGP router not supporting this attribute can still receive routes with this attribute and advertise them to other peers.

Optional non-transitive
• If a BGP router does not support this attribute, it will not advertise routes with this attribute.

The usage of each BGP path attribute is described in the following table.

**Table 47 BGP path attributes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORIGIN</td>
<td>Well-known mandatory</td>
</tr>
<tr>
<td>AS_PATH</td>
<td>Well-known mandatory</td>
</tr>
<tr>
<td>NEXT_HOP</td>
<td>Well-known mandatory</td>
</tr>
<tr>
<td>LOCAL_PREF</td>
<td>Well-known discretionary</td>
</tr>
<tr>
<td>ATOMIC_AGGREGATE</td>
<td>Well-known discretionary</td>
</tr>
<tr>
<td>COMMUNITY</td>
<td>Optional transitive</td>
</tr>
<tr>
<td>MULTI_EXIT_DISC</td>
<td>Optional non-transitive</td>
</tr>
</tbody>
</table>
Usage of BGP path attributes

**ORIGIN**

ORIGIN is a well-known mandatory attribute, which defines the origin of routing information, that is, how a route became a BGP route. It involves three types:

- **IGP**
  - Has the highest priority. Routes added to the BGP routing table using the network command have the IGP attribute.

- **EGP**
  - Has the second highest priority. Routes obtained via EGP have the EGP attribute.

- **Incomplete**
  - Has the lowest priority. The source of routes with this attribute is unknown, which does not mean such routes are unreachable. The routes redistributed from other routing protocols have the incomplete attribute.

**AS_PATH**

AS_PATH is a well-known mandatory attribute. This attribute identifies the autonomous systems through which routing information carried in this Update message has passed. When a route is advertised from the local AS to another AS, each passed AS number is added into the AS_PATH attribute, thus the receiver can determine ASs to route the message back. The number of the AS closest to the receiver’s AS is leftmost, as shown in Figure 48 (page 315).

**Figure 48 AS_PATH attribute**

In general, a BGP router does not receive routes containing the local AS number to avoid routing loops.

**NOTE:** The current implementation supports using the `neighbor allow-as-loop` command to receive routes containing the local AS number.
The AS_PATH attribute can be used for route selection and filtering. BGP gives priority to the route with the shortest AS_PATH length if other factors are the same. As shown in the above figure, the BGP router in AS50 gives priority to the route passing AS40 for sending data to the destination 8.0.0.0.

In some applications, you can apply a routing policy to control BGP route selection by modifying the AS_PATH length.

By configuring an AS path filtering list, you can filter routes based on AS numbers contained in the AS_PATH attribute.

**NEXT_HOP**

Different from IGP, the NEXT_HOP attribute may not be the IP address of a directly connected router. It involves three types of values, as shown in the following figure.

- When advertising a self-originated route to an eBGP peer, a BGP speaker sets the NEXT_HOP for the route to the address of its sending interface.
- When sending a received route to an eBGP peer, a BGP speaker sets the NEXT_HOP for the route to the address of the sending interface.
- When sending a route received from an eBGP peer to an iBGP peer, a BGP speaker does not modify the NEXT_HOP attribute. If load-balancing is configured, the NEXT_HOP attribute will be modified. For load-balancing information, refer to BGP Route Selection.

![Figure 49 NEXT_HOP attribute](image)

**MED (MULTI_EXIT_DISC)**

The MED attribute is exchanged between two neighboring ASs, each of which does not advertise the attribute to any other AS. Similar to metrics used by IGP, MED is used to determine the best route for traffic going into an AS.

When a BGP router obtains multiple routes to the same destination but with different next hops, it considers the route with the smallest MED value the best route if other conditions are the same. As shown below, traffic from AS10 to AS20 travels through Router B that is selected according to MED.
In general, BGP compares MEDs of routes received from the same AS only.

**NOTE:** The current implementation supports using the always-compare-med command to force BGP to compare MED values of routes received from different ASs.

**LOCAL_PREF**

The LOCAL_PREF attribute is exchanged between iBGP peers only, and therefore is not advertised to any other AS. It indicates the priority of a BGP router. LOCAL_PREF is used to determine the best route for traffic leaving the local AS. When a BGP router obtains from several iBGP peers multiple routes to the same destination but with different next hops, it considers the route with the highest LOCAL_PREF value as the best route. As shown below, traffic from AS20 to AS10 travels through Router C that is selected according to LOCAL_PREF.

**COMMUNITY**

The COMMUNITY attribute is used to simplify routing policy usage, and to ease management and maintenance. It identifies a collection of destination addresses having identical attributes, without physical boundaries in between, and having nothing to do with the local AS. Well known community attributes involve:
Internet

By default, all routes belong to the Internet community. Routes with this attribute can be advertised to all BGP peers.

No_Export
After being received, routes with this attribute cannot be advertised out the local AS.

No_Advertise
After being received, routes with this attribute cannot be advertised to other BGP peers.

No_Export_Subconfed
After being received, routes with this attribute cannot be advertised out the local AS.

BGP route selection

Route selection rules

The current BGP implementation supports the following route selection sequence:

- Prefer the route with the lowest Administrative Distance.
- Prefer the route with the larger weight.
- Prefer the route with the highest LOCAL_PREF value.
- Prefer the path that was locally originated via a network or through redistribution from an IGP.
- Prefer the route with the shortest path, excluding confederation segments.
- Prefer the route with the “best” ORIGIN. IGP is better than EGP, which is better than Incomplete.
- If bgp always-compare-med is not configured, prefer any routes that do not have an inferior MED. If bgp always-compare-med has been configured, prefer the route with the lowest MED.
- Prefer the route with the lowest IGP cost to the BGP next hop. IGP cost is determined by comparing the preference, then the weight, then the metric, and finally the metric2 of the two resolving routes.
- If “ip load-sharing” is enabled, BGP inserts up to n most recently received paths in the IP routing table. This allows eBGP multipath load sharing. The maximum value of n is currently 4. The default value of n, when “ip load-sharing” is disabled, is 1. The oldest received path is marked as the best path in the output of show ip bgp prefix/len.
- Prefer routes received from external peers.
- If bgp tie-break-on-age has been specified, prefer the older route.
- If bgp bestpath compare-router-id has been specified, prefer the route learned with the lowest router ID. The router ID is taken from the Open message of the peering session over which the route was received, unless bgp bestpath compare-originator-id has been specified, and the route was received with an ORIGIN_ID. In the latter case, the ORIGIN_ID is used instead of the router ID from the Open message.
- If bgp bestpath compare-cluster-list-length has been specified, prefer the route with the lowest CLUSTER_LIST length.
- Prefer the route with the lowest neighbor address.

**NOTE:** CLUSTER_IDs of route reflectors form a CLUSTER_LIST. If a route reflector receives a route that contains its own CLUSTER ID in the CLUSTER_LIST, the router discards the route to avoid routing loops.
Recursive route in iBGP

The next hop of an iBGP route may not always be directly connected. One of the reasons is next hops in routing information exchanged between iBGP are not modified. In this case, the BGP router needs to find the directly connected next hop via IGP. The matching route with the direct next hop is called the recursive route. The process of finding a recursive route is route recursion.

Route selection with BGP load sharing

BGP differs from IGP in the implementation of load balancing in the following:

- IGP routing protocols such as RIP and OSPF compute metrics of routes, and then implement load sharing over routes with the same metric and to the same destination. The route selection criterion is metric.
- BGP has no route computation algorithm, so it cannot implement load sharing according to metrics of routes. However, BGP has abundant route selection rules, through which it selects available routes for load sharing and adds load sharing to route selection rules.

**NOTE:**

- BGP implements load sharing only on routes that have the same WEIGHT, LOCAL_PREF, ORIGIN, AS_PATH, MED and IGP COST.
- BGP load sharing is applicable between eBGP peers and between iBGP peers.
- If multiple routes to the same destination are available, BGP selects the configured number of routes for load sharing. The maximum number of routes for load sharing is currently 4. Load sharing is enabled by default.

**Figure 52 Network diagram for BGP load sharing**

In Figure 52 (page 319), Router D and Router E are iBGP peers of Router C. Router A and Router B both advertise a route destined for the same destination to Router C. If load sharing is configured and the two routes have the same AS_PATH attribute, ORIGIN attribute, LOCAL_PREF and MED, Router C installs both the two routes to its route table for load sharing. After that, Router C forwards to Router D and Router E the route that has AS_PATH unchanged but has NEXT_HOP changed to Router C; other BGP transitive attributes are those of the best route.
BGP route advertisement rules

The current BGP implementation supports the following route advertisement rules:

- When multiple feasible routes to a destination exist, the BGP speaker advertises only the best route to its peers.
- A BGP speaker advertises only routes used by itself.
- A BGP speaker advertises routes learned from an eBGP peer to all its peers, both eBGP and iBGP.
- A BGP speaker does not advertise routes learnt from an iBGP peer to its other iBGP peers.
- A BGP speaker advertises routes learnt from iBGP to eBGP peers. Note that BGP and IGP synchronization is disabled always and those routes are advertised to eBGP peers directly.

Protocols and standards

- RFC 4271: A Border Gateway Protocol 4 (BGP-4)
- RFC 3392: Capabilities Advertisement with BGP-4
- RFC 2918: Route Refresh Capability for BGP-4
- RFC 1997: BGP Communities Attribute
- RFC 2796: BGP Route Reflection
- RFC 4724: Graceful Restart Mechanism for BGP

BGP extensions

Route reflection

iBGP peers by design do not advertise iBGP routes to other iBGP peers. In order that iBGP peers learn all the routes within the autonomous system and all the external routes, the iBGP peers would have to be fully meshed. This means for n iBGP peers there would have to be n*(n-1)/2 iBGP sessions. In a large autonomous system this could present a challenge in network configuration.

Route Reflection is one of the alternate solutions to alleviate this problem. In the BGP network one of the iBGP speakers is designated as the route reflector which advertises the routes it learns to other iBGP peers.

In a route reflector configuration the other iBGP peers are classified as client peers and non-client peers.

The action taken by the route reflector (after determining the best route) depends on whether the best route was received from a client peer or a non-client peer. If the route was received from a client peer the route reflector will reflect that route to all the client peers and to the non-client peers as well.

If the route was received from a non-client peer then the route is advertised to all its configured clients.

Route reflection introduces two new discretionary attributes: Originator ID and Cluster List, which are used in determining the best path as defined in “BGP route selection” (page 318).

In an Autonomous System more than one route reflector can be configured.

BGP graceful restart (GR)

When a BGP speaker shuts down, planned or unplanned, the routes that are advertised by the speaker and reachable via the speaker now become unreachable. Upon detecting that the BGP speaker has restarted, the peers delete the routes and re-add them when the restarting router advertises them again. This results in route-flap across the BGP connectivity and impacts multiple routing domains causing transient instability in the network.
The Graceful Restart capability is supported as a ‘helper router’ on the HP 3500, 5400, and 8200 product series. In ‘helper only’ mode the router helps the other restarting router by holding the received routes from it as stale routes and not dropping them.

On the HP 8200 product series, the Graceful Restart capability is supported as a restarting router in non-stop routing mode.

1. To establish a BGP session with a peer, a BGP GR Restarter sends an OPEN message with GR capability to the peer.
2. Upon receipt of this message, the peer is aware that the sending router is capable of Graceful Restart, and sends an OPEN message with GR Capability to the GR Restarter to establish a GR session. If neither party has the GR capability, the session established between them will not be GR capable.
3. The GR session between the GR Restarter and its peer goes down when the GR Restarter re-starts BGP. The GR capable peer will mark all routes associated with the GR Restarter as stale. However, during the configured GR Time, it still uses these routes for packet forwarding.
4. After the restart, the GR Restarter will re-establish a GR session with its peer and send a new GR message notifying the completion of restart. Routing information is exchanged between them for the GR Restarter to create a new routing table and forwarding table with stale routing information removed. Then the BGP routing convergence is complete.

Route refresh

When the inbound policy-filter for a peer changes, the routes advertised by the peer must be presented to the policy-filter engine to take effect. This means that all the routes that were received from a peer will have to be preserved in the router and this would raise the demand on memory and CPU resources of the router. The route refresh capability allows the router to request the peer to re-advertise the routes thereby avoiding the requirement to keep a copy of all the routes that were received from all the peers.

BGP configuration task list

The following steps allow for various features of BGP.

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring BGP connection</td>
<td>Required</td>
</tr>
<tr>
<td>Controlling route distribution and reception</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring BGP route redistribution</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring BGP route distribution</td>
<td>Optional</td>
</tr>
<tr>
<td>Filtering policies</td>
<td></td>
</tr>
<tr>
<td>Configuring BGP route reception</td>
<td>Optional</td>
</tr>
<tr>
<td>Filtering policies</td>
<td></td>
</tr>
<tr>
<td>Routingmap filtering and route modifications</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring BGP route attributes</td>
<td>Optional</td>
</tr>
<tr>
<td>Tuning and optimizing BGP networks</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring BGP community</td>
<td>Optional</td>
</tr>
<tr>
<td>Configuring BGP GR</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Configuring BGP connection

This section describes BGP basic configuration.
NOTE: Since BGP runs on TCP, you need to specify the IP addresses of peers, to establish a bgp session. The peers may not be directly connected. In general, IP addresses of loopback interfaces are used to improve stability of BGP connections.

Prerequisites
The neighboring nodes are accessible to each other at the network layer.

Creating a BGP connection
A router ID is the unique identifier of a BGP router in an AS.

- To ensure the uniqueness of a router ID and enhance network reliability, you can specify in BGP configuration context the IP address of a local loopback interface as the router ID.
- If no router ID is specified in BGP context, the global router ID is used.
- If the global router ID is used and then it is removed, the system will select a new router ID. Unconfiguring the router ID in BGP context can make the system select a new router ID.

Follow these steps to create a BGP connection:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>router bgp as-number</td>
<td>Not enabled by default</td>
</tr>
<tr>
<td>Enable BGP</td>
<td>enable</td>
<td></td>
</tr>
<tr>
<td>Specify a BGP Router ID</td>
<td>bgp router-id ip-address</td>
<td>Optional. By default, the global router ID is used.</td>
</tr>
<tr>
<td>Specify a neighbor and its AS number</td>
<td>neighbor ip-address remote-as as-number</td>
<td>Required</td>
</tr>
<tr>
<td>Configure a description for a neighbor</td>
<td>neighbor ip-address description description-text</td>
<td>Optional. Not configured by default</td>
</tr>
</tbody>
</table>

CAUTION: Since a router can reside in only one AS, the router can run only one BGP process.

Specifying the source interface for TCP connections
BGP uses TCP as the transport layer protocol. By default, BGP uses the output interface of the optimal router to a peer as the source interface for establishing TCP connections to the peer. If a BGP router has multiple links to a peer, when the source interface fails, BGP has to reestablish TCP connections, causing network oscillation. Therefore, it is recommended to use a loopback interface as the source interface to enhance stability of BGP connections.

Follow these steps to specify the source interface of TCP connections:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>bgp as-number</td>
<td></td>
</tr>
<tr>
<td>Specify the source interface for establishing TCP connections to a neighbor.</td>
<td>neighbor ip-address update-source ip-address</td>
<td>Required. By default, BGP uses the outbound interface of the best route to the BGP peer as the source interface</td>
</tr>
</tbody>
</table>
Establishing MD5 authentication for TCP connections

BGP requires TCP as the transport protocol. To enhance security, you can configure BGP to perform MD5 authentication when establishing a TCP connection. The two parties must have the same password configured to establish TCP connections. BGP MD5 authentication is not for BGP packets, but for TCP connections. If the authentication fails, no TCP connection can be established.

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>for establishing a TCP connection to the peer.</td>
</tr>
<tr>
<td>Enter BGP view</td>
<td>bgp as-number</td>
<td></td>
</tr>
<tr>
<td>Enable MD5 authentication when establishing a TCP connection to the peer/peer group</td>
<td>peer [[group-name]</td>
<td>[ip-address]] password[ [cipher]</td>
</tr>
</tbody>
</table>

Allowing establishment of eBGP connection to a non-directly connected peer

In general, direct physical links should be available between eBGP peers. If not, you can use the neighbor ip-address ebgp-multihop command to establish a TCP connection over multiple hops between two peers.

Follow these steps to allow establishment of eBGP connection to a non directly connected peer:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>bgp as-number</td>
<td></td>
</tr>
<tr>
<td>Allow the establishment of eBGP connection to a non-directly connected peer</td>
<td>neighbor ip-address ebgp-multihop [hop-count]</td>
<td>Optional. hop-count is 1 by default for eBGP peers</td>
</tr>
</tbody>
</table>

Controlling route distribution, reception and advertisement

Prerequisites

Before configuring this task, you should have completed BGP basic configuration.

Configuring BGP Route Redistribution

You can redistribute IGP routes into BGP rather than self-finding. During route redistribution, BGP can filter routing information from specific routing protocols.

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>router bgp as-number</td>
<td></td>
</tr>
<tr>
<td>Redistribute from other protocols</td>
<td>redistribute static</td>
<td>connected</td>
</tr>
</tbody>
</table>
NOTE: The ORIGIN attribute of routes redistributed using the import-route command is Incomplete. The ORIGIN attribute of networks advertised into the BGP routing table with the network command is IGP. These networks must exist in the local IP routing table, and using a routing policy makes routes control more flexible.

Configuring BGP route inbound and outbound filtering policies

Follow these steps to configure BGP route reception filtering policies:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global Configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>bgp as-number</td>
<td></td>
</tr>
<tr>
<td>Apply filter policy on the inbound or the outbound for each peer</td>
<td>neighbor ip-address route-map route-map-name [in</td>
<td>out]</td>
</tr>
</tbody>
</table>

⚠️ CAUTION: Only routes permitted by the specified filtering policies can be installed into the local BGP routing table.

Configuring BGP route attributes

Prerequisites

Before configuring this task, you should have configured BGP basic functions.

Configuration procedure

You can configure BGP route attributes to influence BGP route selection.

Follow these steps to configure BGP route attributes:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>bgp as-number</td>
<td></td>
</tr>
<tr>
<td>Configure preferences for external, internal, local routes</td>
<td>preference {external-preference internal-preference local-preference}</td>
<td>Optional. The default preferences of external, internal, and local routes are 20, 200, and 200 respectively.</td>
</tr>
<tr>
<td>Configure weight to be assigned to received routes from a peer</td>
<td>neighbor {ip-address} weight {weight}</td>
<td>Optional</td>
</tr>
<tr>
<td>Specify the router as the next hop of routes sent to a peer</td>
<td>neighbor {ip-address} next-hop-self</td>
<td>Optional. By default, advertisements to an eBGP peer take the router as the next hop, while advertisements to an iBGP peer do not take the local router as the next hop.</td>
</tr>
</tbody>
</table>

Configure the AS_PATH attribute:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure repeating times of local AS number in routes from a peer</td>
<td>neighbor {ip-address} allow-as-in [number]</td>
<td>Optional. The local AS number cannot be repeated in routes from the peer.</td>
</tr>
<tr>
<td>Specify a fake AS number for a peer</td>
<td>neighbor {ip-address} local-as as-number</td>
<td>Optional. Not specified by default. This command is only applicable to an eBGP peer.</td>
</tr>
</tbody>
</table>
### CAUTION:

- Using a routing policy can set preferences for routes matching it. Routes not matching it use the default preferences.
- If other conditions are identical, the route with the smallest MED value is selected as the best external route.
- Using the `neighbor next-hop-self` command can specify the router as the next hop for routes sent to a peer. If BGP load balancing is configured, the router specify itself as the next hop for routes sent to a peer regardless of whether the `neighbor next-hop-self` command is configured.
- In a “third party next hop” network, that is, a BGP router has two eBGP peers in a common broadcast subnet, the BGP router does not specify itself as the next hop for routes sent to such an eBGP peer, unless the `neighbor next-hop-self` command is configured.
- In general, BGP checks whether the AS_PATH attribute of a route from a peer contains the local AS number. If so, it discards the route to avoid routing loops.
- You can specify a fake AS number to hide the real one as needed. The fake AS number applies to routes sent to eBGP peers only, that is, eBGP peers in other ASs can only find the fake AS number.
- The `neighbor as-override` command is used only in specific networking environments. Inappropriate use of the command may cause routing loops.

### Tuning and optimizing BGP networks

#### Prerequisites

BGP connections have been created.

#### Configuring BGP keepalive interval and holdtime

After establishing a BGP connection, two routers send keepalive messages periodically to each other to keep the connection. If a router receives no keepalive or update message from the peer within the holdtime, it tears down the connection.

If two parties have the same timer assigned with different values, the smaller one is used by the two parties.

Follow these steps to configure BGP keepalive interval and holdtime:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>bgp as-number</td>
<td></td>
</tr>
</tbody>
</table>
### Remarks

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the global keepalive interval and holdtime</td>
<td>timers {keepalive-time} {hold-time}</td>
<td></td>
</tr>
<tr>
<td>Configure the keepalive interval and holdtime for a peer</td>
<td>neighbor {ip-address} timers {keepalive-time} {hold-time}</td>
<td>Optional. By default, the keepalive interval is 60 seconds, and holdtime is 180 seconds.</td>
</tr>
</tbody>
</table>

#### CAUTION:
- The maximum keepalive interval should be one third of the holdtime and no less than 1 second. The holdtime is no less than 3 seconds unless it is set to 0.
- The intervals set with the neighbor timers command are preferred to those set with the timers command.
- If the router has established a neighbor relationship with a peer, you need to reset the BGP connection to validate the new set timers.

### Configuring a large scale BGP network

In a large-scale BGP network, configuration and maintenance become difficult due to large numbers of BGP peers. To facilitate configuration in this case, you can configure community or route reflector as needed.

#### Configuration prerequisites

Follow these steps to configure BGP community:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>bgp as-number</td>
<td></td>
</tr>
<tr>
<td>Advertise the community attribute to a peer</td>
<td>neighbor {ip-address} send-community</td>
<td>Enabled by default</td>
</tr>
</tbody>
</table>

#### CAUTION: When configuring BGP community, you need to configure a routing policy to define the community attribute, and apply the routing policy to route advertisement.

### Configuring a BGP route reflector

Follow these steps to configure a BGP route reflector:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global configuration context</td>
<td>configuration</td>
<td></td>
</tr>
<tr>
<td>Enter BGP context</td>
<td>bgp as-number</td>
<td></td>
</tr>
<tr>
<td>Configure the router as a route reflector and specify a peer as its client</td>
<td>client-to-client-reflection</td>
<td>Enabled by default</td>
</tr>
<tr>
<td>Enable route reflection between clients</td>
<td>neighbor {ip-address} route-reflector-client</td>
<td>Optional. Enabled by default.</td>
</tr>
</tbody>
</table>
**CAUTION:** In general, it is not required to make clients of a route reflector fully meshed. The route reflector forwards routing information between clients. If clients are fully meshed, you can disable route reflection between clients to reduce routing costs.

In general, a cluster has only one route reflector, and the router ID is used to identify the cluster. You can configure multiple route reflectors to improve network stability. In this case, you need to specify the same cluster ID for these route reflectors to avoid routing loops.

### Configuring BGP graceful restart

Perform the following configuration on the GR Restarter and GR Helper respectively.

**NOTE:** A device can act as both the GR Restarter and GR Helper at the same time.

Follow these steps to configure BGP GR:

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter global Configuration context</td>
<td><code>configuration</code></td>
<td></td>
</tr>
<tr>
<td>Enable BGP, and enter its view</td>
<td><code>bgp as-number</code></td>
<td></td>
</tr>
<tr>
<td>Enable BGP, and enter its view</td>
<td><code>bgp graceful-restart</code></td>
<td>Required. Disabled by default.</td>
</tr>
<tr>
<td></td>
<td><code>stalepath-time</code></td>
<td></td>
</tr>
<tr>
<td>Configure the maximum time allowed for the peer to reestablish a BGP session</td>
<td><code>graceful-restart timer</code></td>
<td>Optional. 120 seconds by default.</td>
</tr>
<tr>
<td>Configure the maximum time to wait for the End-of-RIB marker</td>
<td><code>graceful-restart timer</code></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:** In general, the maximum time allowed for the peer (the GR restarter) to reestablish a BGP session should be less than the Holdtime carried in the OPEN message. The End-Of-RIB (End of Routing-Information-Base) indicates the end of route updates.

### Displaying and maintaining BGP

### Displaying BGP

<table>
<thead>
<tr>
<th>To do...</th>
<th>Use the command...</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about BGP routes installed in the BGP routing information base (RIB)</td>
<td><code>show ip bgp</code></td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display specific information on the route and the BGP path attributes of the route</td>
<td><code>show ip bgp ipv4-addr/masklen</code></td>
<td></td>
</tr>
<tr>
<td>Display generic global configuration information regarding BGP</td>
<td><code>show ip bgp general</code></td>
<td></td>
</tr>
<tr>
<td>Display detailed information on the route if the route’s AS_PATH information matches the supplied regular expression</td>
<td><code>show ip bgp ipv4-addr/masklen regexp aspath-reg-ex</code></td>
<td></td>
</tr>
<tr>
<td>Display all the routes in the IP routing table, including BGP routes</td>
<td><code>show ip route</code></td>
<td></td>
</tr>
<tr>
<td>To do...</td>
<td>Use the command...</td>
<td>Remarks</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Display only the BGP routes in the IP routing table</td>
<td>show ip route bgp [ip4-addr]</td>
<td></td>
</tr>
<tr>
<td>Display the routes whose community information matches the supplied community numbers and also the AS_PATH information matches the supplied regular expression</td>
<td>show ip bgp community comm-num... regexp aspath-reg-ex</td>
<td></td>
</tr>
<tr>
<td>Display the routes whose community information matches exactly the supplied community numbers and also whose AS_PATH information matches the supplied regular expression</td>
<td>show ip bgp community comm-num... exact regexp aspath-reg-ex</td>
<td></td>
</tr>
<tr>
<td>Display all routes whose AS_PATH matches the regular-expression given</td>
<td>show ip bgp regex reg-ex</td>
<td></td>
</tr>
<tr>
<td>Display basic route information (destination and nexthop) and the communities tagged to the route in full</td>
<td>show ip bgp [ip4-addr</td>
<td>masklen[longer-prefix]] route community</td>
</tr>
<tr>
<td>Display BGP peer information</td>
<td>show ip bgp neighbor [ip4-addr]</td>
<td></td>
</tr>
<tr>
<td>Display in brief the BGP neighbor information</td>
<td>show ip bgp summary</td>
<td></td>
</tr>
<tr>
<td>Display the list of AS_PATH that BGP has learnt from the routing information it has received</td>
<td>show ip bgp as-path</td>
<td></td>
</tr>
<tr>
<td>Display the list of protocols whose routes are being redistributed into BGP</td>
<td>show ip bgp redistribute</td>
<td></td>
</tr>
</tbody>
</table>

**BGP configuration examples**

**BGP basic configuration**

**Network requirements**

In the following network, run eBGP between Switch A and Switch B and iBGP between Switch B and Switch C so that Switch C can access the network 8.1.1.0/24 connected to Router A.

**Figure 53 Network diagram for BGP basic configuration**

![Network diagram](image_url)

**Configuration procedure**

1. Configure IP addresses for interfaces (omitted).
2. Configure iBGP.
   - To prevent route flapping caused by port state changes, this example uses loopback interfaces to establish iBGP connections.
   - Because loopback interfaces are virtual interfaces, you need to use the peer connect-interface command to specify the loopback interface as the source interface for establishing BGP connections.
   - Enable OSPF in AS 65009 to ensure that Switch B can communicate with Switch C through loopback interfaces.

```
# Configure Switch B
configuration
[HP Switch] router bgp 65009
HP Switch(bgp)# bgp router-id 2.2.2.2
HP Switch(bgp)# neighbor 3.3.3.3 remote-as 65009
HP Switch(bgp)# exit
HP Switch(config)# router ospf
HP Switch(ospf)# enable
HP Switch(ospf)# area 0
HP Switch(ospf)# network 2.2.2.2/32
HP Switch(ospf)# network 9.1.1.1/24
HP Switch(ospf)# exit
HP Switch(config)# vlan 300
HP Switch(vlan-300)# ip ospf
```

```
# Configure Switch C
configuration
[HP Switch] router bgp 65009
HP Switch(bgp)# bgp router-id 3.3.3.3
HP Switch(bgp)# neighbor 2.2.2.2 remote-as 65009
HP Switch(bgp)# neighbor 2.2.2.2 connect-interface loopback 0
HP Switch(bgp)# exit
[HP Switch] router ospf
HP Switch (ospf)# enable
HP Switch(ospf)# area 0
HP Switch(ospf)# network 3.3.3.3/32
HP Switch(ospf)# network 9.1.1.0/24
HP Switch(ospf)# exit
HP Switch (config)# vlan 300
HP Switch (vlan-300)# ip ospf
HP Switch] show ip bgp summary
Peer Information
Remote Address Remote-AS Local-AS State Admin Status
-------------- --------- -------- ------------ -----
2.2.2.2         65009     65009    Established Start
```

The output information shows that Switch C has established an iBGP peer relationship with Switch B.

3. Configure eBGP.
   - The eBGP peers, Switch A and Switch B (usually belong to different carriers), are located in different ASs. Generally, their loopback interfaces are not reachable to each other, so directly connected interfaces are used for establishing BGP sessions.
   - To enable Switch C to access the network 8.1.1.0/24 connected directly to Switch A, inject network 8.1.1.0/24 to the BGP routing table of Switch A.

```
# Configure Switch A.
configuration
[HP Switch] router bgp 65008
HP Switch(bgp)# bgp router-id 1.1.1.1
HP Switch(bgp)# neighbor 3.1.1.1 remote-as 65009
```
HP Switch(bgp)# network 8.1.1.1/24
HP Switch(bgp)# exit

# Configure Switch B.

[HP Switch] router bgp 65009
HP Switch(bgp)# neighbor 3.1.1.2 remote-as 65008
HP Switch(bgp)# exit

# Show IP bgp peer information on Switch B.

[HP Switch] show ip bgp summary
HP Switch(bgp)# show ip bgp summary
Peer Information
Remote Address  Remote-AS  Local-AS  State    Admin Status
-------------- ---------  --------  --------  ------------
2.2.2.2         65009     65009  Established  Start
3.1.1.2         65008     65009  Established  Start

The output shows that Switch B has established an iBGP peer relationship with Switch C and an eBGP peer relationship with Switch A.

# Display the BGP routing table on Switch A.

[HP Switch] show ip bgp
HP Switch (bgp)# show ip bgp
Local AS : 100
Local Router-id : 20.0.0.1
BGP Table Version : 0
Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Nexthop  Metric LocalPref  Weight AsPath
----------------------------------------------------------
*> 8.1.1.0/24                   0            32768    I
*> 8.1.1.0/24     0.0.0.0       0               0     I

# Display the BGP routing table on Switch B.

[HP Switch] show ip bgp
Local AS : 100
Local Router-id : 20.0.0.1
BGP Table Version : 0
Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Nexthop    Metric LocalPref  Weight AsPath
----------------------------------------------------------
*>e 8.1.1.0/24                0              0    65008i

# Display the BGP routing table on Switch C.

HP Switch (bgp)# show ip bgp
Local AS : 100
Local Router-id : 20.0.0.1
BGP Table Version : 0
Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Nexthop    Metric LocalPref  Weight AsPath
----------------------------------------------------------
*>i 8.1.1.0/24                  0            0    65008i

**NOTE:** From the above outputs, you find Switch A has not learned a route to AS65009, and Switch C has learned network 8.1.1.0 but the next hop 3.1.1.2 is unreachable, so the route is invalid.
4. Redistribute connected routes.
   Configure BGP to redistribute direct routes on Switch B, so that Switch A can obtain the route to 9.1.1.0/24 and Switch C can obtain the route to 3.1.1.0/24.
   
   # Configure Switch B.
   ```
   [HP Switch] router bgp 65009
   HP Switch(bgp)# redistribute connected
   ```
   
   # Display the BGP routing table on Switch A.
   ```
   [HP Switch] show ip bgp
   Local AS : 65009
   Local Router-id : 1.1.1.1
   
   BGP Table Version : 0
   Status codes: * - valid, > - best, i - internal, e - external, s - stale
   
   Origin codes: i - IGP, e - EGP, ? - incomplete
   
<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric LocalPref Weight AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>*e 2.2.2.2/32</td>
<td>3.1.1.1</td>
<td>0</td>
</tr>
<tr>
<td>*e 3.1.1.0/24</td>
<td>3.1.1.1</td>
<td>0</td>
</tr>
<tr>
<td>*e 8.1.1.0/24</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>*e 8.1.1.0/24</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
   
   Two routes 2.2.2.2/32 and 9.1.1.0/24 have been added in Switch A's routing table.
   
   # Display the BGP routing table on Switch C.
   ```
   [HP Switch] show ip bgp
   Local AS : 65009
   Local Router-id : 3.3.3.3
   
   BGP Table Version : 1
   Status codes: * - valid, > - best, i - internal, e - external, s - stale
   
   Origin codes: i - IGP, e - EGP, ? - incomplete
   
<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric LocalPref Weight AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>*e 2.2.2.2/32</td>
<td>9.1.1.1</td>
<td>0</td>
</tr>
<tr>
<td>*e 3.1.1.0/24</td>
<td>9.1.1.1</td>
<td>0</td>
</tr>
<tr>
<td>*e 8.1.1.0/24</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>*e 9.1.1.0/24</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>*e 9.1.1.0/24</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
   
   Route 8.1.1.0 becomes valid with the next hop as Switch A.
   
   5. Verification.

   **Route filter configuration**

   **Network requirements**

   In the following figure, Switch B establishes eBGP connections with Switch A and C. Configure No.Export community attribute on Switch A to make routes from AS 10 not advertised by AS 20 to any other AS.
Configuration procedure

1. Configure IP addresses for interfaces (omitted).
2. Configure eBGP.

   # Configure Switch A.
   
   configuration
   
   [HP Switch] router bgp 10
   HP Switch(bgp)# bgp router-id 1.1.1.1
   HP Switch(bgp)# neighbor 200.1.2.2 remote-as 20
   HP Switch(bgp)# network 9.1.1.0/255.255.255.0/8
   HP Switch(bgp)# exit

   # Configure Switch B.
   
   configuration
   
   [HP Switch] bgp 20
   HP Switch(bgp)# bgp router-id 2.2.2.2
   HP Switch(bgp)# neighbor 200.1.2.1 remote-as 10
   HP Switch(bgp)# neighbor 200.1.3.2 remote-as 30
   HP Switch(bgp)# exit

   # Configure Switch C.
   
   configuration
   
   [HP Switch] bgp 30
   HP Switch(bgp)# bgp router-id 3.3.3.3
   HP Switch(bgp)# neighbor 200.1.3.1 remote-as 20
   HP Switch(bgp)# exit

   # Display the BGP routing table on Switch B.
   
   [HP Switch] show ip bgp 9.1.1.0
   Local AS : 20 Local Router-id : 2.2.2.2
   BGP Table Version : 3

   Network : 9.1.1.0/24       Nexthop         : 200.1.2.1
   Peer   : 200.1.2.1          Origin          : igp
   Metric : 0                  Local Pref      :
   Weight : 0                  Calc. Local Pref : 100
   Valid  : Yes                Type            : external
   Stale  : No
   Best   : Yes (Only Route Available)
   AS-Path : 100
   Communities :

   Switch B advertised routes to Switch C in AS30.

   # Display the routing table on Switch C.
[HP Switch] show ip bgp

Local AS : 30
Local Router-id : 3.3.3.3

BGP Table Version : 1
Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next-hop Metric LocalPref Weight AsPath
-------------------------------------------------------
> *i 9.1.1.0/24 200.1.3.1 0 100 10i

Switch C learned route 9.1.1.0/24 from Switch B.

3. Configure BGP community.

# Configure a routing policy.

route-map bgp-out permit seq 10
HP Switch (route-map-bgp-out)# set community no-export
HP Switch (route-map-bgp-out)# exit

# Apply the routing policy.

[HP Switch] bgp 10
HP Switch(bgp)# neighbor 200.1.2.2 route-map bgp-out out

# Display the route on Switch B.

[HP Switch] show ip bgp 9.1.1.0/24

Local AS : 20 Local Router-id : 2.2.2.2
BGP Table Version : 3

Network : 9.1.1.0/24 Next-hop : 200.1.2.1
Peer : 200.1.2.1 Origin : igp Metric : 0 Local Pref : Weight
Calc. Local Pref : 100
Valid : Yes Type : external
Stale : No
Best : Yes (Only Route Available) AS-Path : 100
Communities: no-export

# Display the routing table on Switch C.

HP Switch # show ip bgp 9.1.1.0/24

The route 9.1.1.0/24 is not available in the routing table of Switch C.

BGP route reflector configuration

Network requirements

In the following figure, all switches run BGP.

- Between Switch A and Switch B is an eBGP connection, between Switch C and Switch B, and between Switch C and Switch D are iBGP connections.
- Switch C is a route reflector with clients Switch B and D.
- Switch D can learn route 1.0.0.0/8 from Switch C.
Configuration procedure

1. Configure IP addresses for interfaces (omitted).
2. Configure BGP connections.
   
   # Configure Switch A.
   configuration
   [HP Switch] router bgp 100
   HP Switch(bgp)# bgp router-id 1.1.1.1
   HP Switch(bgp)# neighbor 192.1.1.2 remote-as 200
   # Inject network 1.0.0.0/8 to the BGP routing table.
   HP Switch(bgp)# network 1.0.0.0
   HP Switch(bgp)# exit

   # Configure Switch B.
   HP Switch(bgp)# configuration
   [HP Switch] router bgp 200
   HP Switch(bgp)# bgp router-id 2.2.2.2
   HP Switch(bgp)# neighbor 192.1.1.1 remote-as 100
   HP Switch(bgp)# neighbor 193.1.1.1 remote-as 200
   HP Switch(bgp)# neighbor 193.1.1.1 next-hop-self
   HP Switch(bgp)# exit

   # Configure Switch C.
   configuration
   [HP Switch] router bgp 200
   HP Switch(bgp)# bgp router-id 3.3.3.3
   HP Switch(bgp)# neighbor 193.1.1.2 remote-as 200
   HP Switch(bgp)# neighbor 194.1.1.2 remote-as 200
   HP Switch(bgp)# exit

   # Configure Switch D.
   configuration
   [HP Switch] router bgp 200
   HP Switch(bgp)# bgp router-id 4.4.4.4
   HP Switch(bgp)# neighbor 194.1.1.1 remote-as 200
   HP Switch(bgp)# exit

3. Configure the route reflector.
   
   # Configure Switch C.
   [HP Switch] router bgp 200
   HP Switch(bgp)# neighbor 193.1.1.2 route-reflector-client
   HP Switch(bgp)# neighbor 194.1.1.2 route-reflector-client
   HP Switch(bgp)# exit
4. Verify the above configuration.

# Display the BGP routing table on Switch B.

[HP Switch] show ip bgp
Local AS : 200
Local Router-id : 200.1.2.2

BGP Table Version : 1
Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt;i 1.0.0.0/24</td>
<td>200.1.3.1</td>
<td>0</td>
<td>0</td>
<td>100i</td>
<td></td>
</tr>
</tbody>
</table>

# Display the BGP routing table on Switch D.

[HP Switch] show ip bgp
Local AS : 200
Local Router-id : 200.1.2.2

BGP Table Version : 1
Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt;e 1.0.0.0/24</td>
<td>200.1.3.1</td>
<td>0</td>
<td>100</td>
<td>100i</td>
<td></td>
</tr>
</tbody>
</table>

Switch D learned route 1.0.0.0/8 from Switch C.

BGP path selection configuration

Network requirements

- In the figure below, all switches run BGP. Between Switch A and Switch B, and between Switch A and Switch C are eBGP connections. Between Switch B and Switch D, and between Switch D and Switch C are iBGP connections.
- OSPF is the IGP protocol in AS 200.
- Configure routing policies, making Switch D use the route 1.0.0.0/8 from Switch C as the optimal.

Figure 56 Network diagram for BGP path selection configuration

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
<th>Device</th>
<th>Interface</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch A</td>
<td>Vlan101</td>
<td>1.0.0.0/8</td>
<td>Switch D</td>
<td>Vlan400</td>
<td>195.11.1/24</td>
</tr>
<tr>
<td></td>
<td>Vlan100</td>
<td>192.1.1/24</td>
<td></td>
<td>Vlan300</td>
<td>194.1.1/24</td>
</tr>
<tr>
<td></td>
<td>Vlan200</td>
<td>193.1.1/24</td>
<td></td>
<td>Vlan400</td>
<td>195.1.1.2/24</td>
</tr>
</tbody>
</table>
Configuration procedure

1. Configure IP addresses for interfaces (omitted).

2. Configure OSPF on Switch B, C, and D.

   # Configure Switch B.
   
   configuration
   [HP Switch] ospf
   HP Switch(ospf)# area 0
   HP Switch(ospf)# network 192.1.1.0/ 0.0.0.255
   HP Switch(ospf)# network 194.1.1.0/ 0.0.0.255
   HP Switch(ospf)# exit
   HP Switch(ospf)# exit

   # Configure Switch C.
   
   configuration
   [HP Switch] router ospf
   HP Switch (ospf)# enable
   HP Switch(ospf)# area 0
   HP Switch(ospf)# network 193.1.1.0/ 0.0.0.255
   HP Switch(ospf)# network 195.1.1.0/ 0.0.0.255
   HP Switch(ospf)# exit
   HP Switch(ospf)# exit

   # Configure Switch D.
   
   configuration
   [HP Switch] router ospf
   HP Switch (ospf)# enable
   HP Switch(ospf)# area 0
   HP Switch(ospf)# network 194.1.1.0/ 0.0.0.255
   HP Switch(ospf)# network 195.1.1.0/ 0.0.0.255
   HP Switch(ospf)# exit
   HP Switch(ospf)# exit

3. Configure BGP connections.

   # Configure Switch A.
   
   configuration
   [HP Switch] router bgp 100
   HP Switch(bgp)# neighbor 192.1.1.2 remote-as 200
   HP Switch(bgp)# neighbor 193.1.1.2 remote-as 200

   # Inject network 1.0.0.0/8 to the BGP routing table on Switch A.
   HP Switch(bgp)# network 1.0.0.0/8
   HP Switch(bgp)# exit

   # Configure Switch B.
   
   [HP Switch] router bgp 200
   HP Switch(bgp)# neighbor 192.1.1.1 remote-as 100
   HP Switch(bgp)# neighbor 194.1.1.1 remote-as 200
   HP Switch(bgp)# exit

   # Configure Switch C.
   
   [HP Switch] router bgp 200
   HP Switch(bgp)# neighbor 193.1.1.1 remote-as 100
   HP Switch(bgp)# neighbor 195.1.1.1 remote-as 200
   HP Switch(bgp)# exit

   # Configure Switch D.
[HP Switch] router bgp 200
HP Switch(bgp)# neighbor 194.1.1.2 remote-as 200
HP Switch(bgp)# neighbor 195.1.1.2 remote-as 200
HP Switch(bgp)# exit
4. Configure attributes for route 1.0.0.0/8, making Switch D give priority to the route learned from Switch C.
   - Configure a higher MED value for the route 1.0.0.0/8 advertised from Switch A to peer 192.1.1.2.

   # Define a prefix-list to permit route 1.0.0.0/8.
   HP Switch (config)# ip prefix-list pl_1 permit 1.0.0.0/24

   # Define two routing policies, apply_med_50, which sets the MED for route 1.0.0.0/8 to 50, and apply_med_100, which sets the MED for route 1.0.0.0/8 to 100.

   # HP Switch] route-map apply_med_50 permit
   HP Switch (route-map-apply_med_50)# match ip address prefix-list pl_1
   HP Switch (route policy)# set metric 50
   [HP Switch] route-map apply_med_50 permit seq 20
   HP Switch (route policy)# exit

   # HP Switch] route-map apply_med_100 permit
   HP Switch (route-map-apply_med_100)# match ip address prefix-list pl_1
   HP Switch (route policy)# set metric 100
   HP Switch (route policy)# route-map apply_med_100 permit seq 20
   HP Switch (route policy)# exit

   # Apply routing policy apply_med_50 to the route advertised to peer 193.1.1.2 (Switch C), and apply_med_100 to the route advertised to peer 192.1.1.2 (Switch B).

   # HP Switch] bgp 100
   HP Switch(bgp)# neighbor 193.1.1.2 route-map apply_med_50 out
   HP Switch(bgp)# neighbor 192.1.1.2 route-policy apply_med_100 out
   HP Switch(bgp)# exit

   # Display the BGP routing table on Switch D.
   [HP Switch] show ip bgp

   Local AS : 100
   Local Router-id : 194.1.1.1

   BGP Table Version : 1

   Status codes: * - valid, > - best, i - internal, e - external, s - stale
   Origin codes: i - IGP, e - EGP, ? - incomplete

   Network        Nexthop    Metric LocalPref Weight AsPath
   ----------------------------------------------
   *>e 1.0.0.0/24 194.1.1.2       50            0     100i
   *>e 1.0.0.0/24 195.1.1.2      100            0     100i

   You can find route 1.0.0.0/8 is the optimal.

   - Configure different local preferences on Switch B and C for route 1.0.0.0/8, making Switch D give priority to the route from Switch C.

   # Define an ip prefix-list on Router C, permitting route 1.0.0.0/8.
   HP Switch (config) # ip prefix-list pl_1 permit 1.0.0.0/8

   # Configure a routing policy named localpref on Switch C, setting the local preference of route 1.0.0.0/8 to 200 (the default is 100).

   # HP Switch] route-map localpref permit seq 10
   HP Switch (route-policy)# match ip address prefix-list pl_1
   HP Switch (route-policy)# set local-preference 200
   HP Switch (route-policy)# route-map localpref permit seq 20

   # Apply routing policy localpref to routes from peer 193.1.1.1.

   # HP Switch] router bgp 200
   HP Switch(bgp)# neighbor 193.1.1.1 route-map localpref in
   HP Switch(bgp)# exit

   # Display the routing table on Switch D.
[HP Switch] show ip bgp
Local AS : 100
Local Router-id : 194.1.1.1

BGP Table Version : 1

Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt;e 1.0.0.0/24</td>
<td>200.1.3.1</td>
<td>200</td>
<td>0</td>
<td>100i</td>
<td></td>
</tr>
<tr>
<td>* i 1.0.0.0/24</td>
<td></td>
<td>100</td>
<td>0</td>
<td>100i</td>
<td></td>
</tr>
</tbody>
</table>

You can find route 1.0.0.0/8 from Switch D to Switch C is the optimal.

BGP GR configuration

Network requirements

In the following figure, all switches are BGP switches. There is a eBGP connection between Switch A and Switch B. Switch B and Switch C are connected over an iBGP connection. Enable GR for BGP so that the communication between Switch A and Switch C is not affected when an active/standby main board switchover occurs on Switch B.

Figure 57 Network diagram for BGP GR configuration

Configuration procedure

1. Configure Switch A.
   # Configure IP addresses for interfaces (omitted).
   # Configure the eBGP connection.
   configuration
   [HP Switch] router bgp 65008
   HP Switch (bgp)# bgp router-id 1.1.1.1
   # Configure BGP GR stalepath-timeout (optional).
   HP Switch (bgp)# bgp graceful-restart stalepath-time 360
   HP Switch (bgp)# neighbor 200.1.1.1 remote-as 65009
   # Inject network 8.0.0.0/8 to the BGP routing table.
   HP Switch (bgp)# network 8.0.0.0/8
   # Enable GR for BGP Peer.
   HP Switch (bgp)# neigh 200.1.1.1 graceful-restart

2. Configure Switch B.
   # Configure IP addresses for interfaces (omitted).
   # Configure the eBGP connection.
   configuration
   HP Switch (bgp)# router bgp 65009
   # Configure BGP GR restart-time and stalepath-timeout (Optional).
   HP Switch (bgp)# bgp graceful-restart restart-time 120
   stalepath-time 360

BGP configuration examples 339
HP Switch (bgp)# bgp router-id 2.2.2.2
HP Switch (bgp)# neighbor 200.1.1.2 remote-as 65008
# Configure the iBGP connection.
HP Switch (bgp)# neighbor 9.1.1.2 remote-as 65009
# Configure BGP to redistribute direct routes.
HP Switch (bgp)# redistribute connected
# Enable GR capability for BGP Peers.
HP Switch (bgp)# neighbor 200.1.1.2 graceful-restart
HP Switch (bgp)# neighbor 9.1.1.2 graceful-restart
# Configure BGP for non-stop forwarding
HP Switch (bgp)# non-stop

3. Configure Switch C.
   # Configure IP addresses for interfaces (omitted).
   configuration
   HP Switch # router bgp 65009
   HP Switch (bgp)# bgp router-id 3.3.3.3
   HP Switch (bgp)# neighbor 9.1.1.1 remote-as 65009
   # Configure BGP to redistribute direct routes.
   HP Switch (bgp)# redistribute connected
   BGP Configuration Example
   # Enable GR for BGP Peer.
   HP Switch (bgp)# neighbor 9.1.1.1 graceful-restart

Verification
After completing the above configuration, perform an active/standby main board switchover on Switch B. Switch A and Switch C can ping each other without any packet drops. Also ensure that there are no flaps of BGP learnt routes on the peer switches.

BGP show routines

Synopsis:

```
show ip bgp [ipv4-addr [mask] [longer-prefixes]]
```

Displays information about BGP routes installed in the BGP routing information base (RIB).

- **ipv4-addr**
  - IP address entered to filter the output to display only a particular host or network in the BGP routing table.

- **mask**
  - Mask to filter or match hosts that are part of the specified network.

- **longer-prefixes**
  - If a prefix is specified, optionally specify to show routes matching the specified Network/Mask pair only.

HP Switch (bgp)# show ip bgp
Local AS : 100             Local Router-id : 10.0.102.138
Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
### Synopsis:

**show ip bgp ipv4-addr/masklen**

Displays specific information on the route and the BGP path attributes of the route.

HP Switch (bgp)# show ip bgp 11.0.0.0/8

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>11.0.0.0/8</td>
<td>10.0.102.153</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>22.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>22.0.0.0/8</td>
<td>10.0.102.198</td>
<td>0</td>
<td>0</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>33.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>200</td>
</tr>
<tr>
<td>33.0.0.0/8</td>
<td>10.0.102.198</td>
<td>0</td>
<td>0</td>
<td>300</td>
<td>400</td>
</tr>
</tbody>
</table>

**Synopsis:**

**show ip bgp ipv4-addr/masklen regexp aspath-reg-ex**

Displays detailed information on the route if the route’s aspath information matches the supplied regular expression. This will filter both on the prefix/len and the regular expression.

HP Switch (bgp)# show ip bgp 11.0.0.0/8 regexp 20

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AS-Path</th>
<th>Communities</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>200</td>
<td>200:20 100:50</td>
</tr>
</tbody>
</table>

**Synopsis:**

**show ip bgp [ipv4-addr]**

Displays all the routes in the IP routing table, including BGP routes.
ipv4-addr

IP address entered to filter the output to display only a particular host or network
in the IP routing table.

HP Switch (bgp)# show ip route

IP Route Entries

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td>10.0.0.1</td>
<td>static</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>DEFAULT_VLAN</td>
<td></td>
<td>connected</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>11.0.0.0/8</td>
<td>10.0.102.153</td>
<td>bgp</td>
<td></td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>22.0.0.0/8</td>
<td>10.0.102.40</td>
<td>bgp</td>
<td></td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>33.0.0.0/8</td>
<td>10.0.102.40</td>
<td>bgp</td>
<td></td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>99.0.0.0/8</td>
<td>DEFAULT_VLAN</td>
<td>static</td>
<td></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>127.0.0.0/8</td>
<td>reject</td>
<td>static</td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>127.0.0.1/32</td>
<td>lo0</td>
<td>connected</td>
<td></td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Synopsis:

show ip route bgp [ipv4-addr]
Displays only the BGP routes in the IP routing table.

ipv4-addr

IP address entered to filter the output to display only a particular host or network
in the BGP routing table.

HP Switch (bgp)# show ip route bgp

IP Route Entries

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>VLAN Type</th>
<th>Sub-Type</th>
<th>Metric</th>
<th>Dist.</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0.0.0/8</td>
<td>10.0.102.153</td>
<td>bgp</td>
<td></td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>22.0.0.0/8</td>
<td>10.0.102.40</td>
<td>bgp</td>
<td></td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>33.0.0.0/8</td>
<td>10.0.102.40</td>
<td>bgp</td>
<td></td>
<td>0</td>
<td>20</td>
</tr>
</tbody>
</table>

Synopsis:

show bgp community comm-nums
Displays the list of routes who have specific communities tagged to them.

HP Switch (bgp)# show ip community 200:20 200:30

Local AS    : 100                    Local Router-id :

Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>* e 11.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>?</td>
</tr>
<tr>
<td>*e &gt; 33.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>?</td>
</tr>
</tbody>
</table>

Synopsis:

show ip bgp community regexp community-reg-ex
Displays the routes whose community information matches the supplied regular expression.
HP Switch (bgp)# show ip bgp community regexp "2"

Local AS : 100        Local Router-id : 10.0.102.138

Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>* e 11.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>200</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>* e 11.0.0.0/8</td>
<td>10.0.102.153</td>
<td>0</td>
<td>200</td>
<td></td>
<td>i</td>
</tr>
<tr>
<td>* e 22.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>200</td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>

Synopsis:

show ip bgp community comm-num... regexp aspath-reg-ex
Displays the routes whose community information matches the supplied community numbers and also the AS_PATH information matches the supplied regular expression.

HP Switch (bgp)# show ip bgp community 20 regexp "2"

Local AS : 100        Local Router-id : 10.0.102.138

Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>* e 11.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>200</td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>

Synopsis:

show ip bgp community comm-num... exact regexp aspath-reg-ex
Displays the routes whose community information matches exactly the supplied community numbers and also whose AS_PATH information matches the supplied regular expression.

HP Switch (bgp)# show ip bgp community 200:20 100:50 exact regexp "2"

Local AS : 100        Local Router-id : 10.0.102.138

Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Metric</th>
<th>LocalPref</th>
<th>Weight</th>
<th>AsPath</th>
</tr>
</thead>
<tbody>
<tr>
<td>* e 11.0.0.0/8</td>
<td>10.0.102.40</td>
<td>0</td>
<td>200</td>
<td></td>
<td>?</td>
</tr>
</tbody>
</table>

Synopsis:

show ip bgp regex reg-ex
Displays all routes whose AS_PATH matches the regular-expression given.

HP Switch (bgp)# show ip bgp regexp "^300"

Local AS : 100        Local Router-id :

Status codes: * - valid, > - best, i - internal, e - external, s - stale
Origin codes: i - IGP, e - EGP, ? - incomplete
<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>* e 22.0.0.0/8 10.0.102.198</td>
<td>0 200:20 100:50</td>
<td>?</td>
</tr>
<tr>
<td>* e 33.0.0.0/8 10.0.102.198</td>
<td>0 100:50</td>
<td>?</td>
</tr>
</tbody>
</table>

**Synopsis:**

show ip bgp [ipv4-addr/masklen [longer-prefix]] route community

Displays basic route information (destination and nexthop) and the communities tagged to the route in full. This show routine is especially helpful when one wants to look at the communities that are tagged to all routes in a glance.

HP Switch (bgp)# show ip bgp 22.0.0.0/8 route community

Local AS : 100

Status codes: * - valid, > - best, i - internal, e - external, s - stale

Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Nexthop</th>
<th>Community</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt;e 22.0.0.0/8 10.0.102.40</td>
<td>200:20 100:50</td>
<td>?</td>
</tr>
<tr>
<td>*e 22.0.0.0/8 10.0.102.198</td>
<td>no-export</td>
<td>?</td>
</tr>
</tbody>
</table>

**Synopsis:**

show ip bgp neighbor [ipv4-addr]

Displays information about the state of BGP's IPv4 peering sessions.

HP Switch (bgp)# show ip bgp neighbor 10.0.102.40

BGP Neighbor 10.0.102.40

BGP Version : 4
Remote Router ID : 10.0.102.40 Local Router ID : 10.0.102.138
Remote-AS : 200 Local-AS : 100
Remote Port : 179 Local Port : 56126
State : Established Up Time : 0h:3m:29s
Admin Status : Start Link Type : External
Conn Established : 1 Conn Dropped : 0
Last Read : 0h:0m:29s Last Write : 0h:0m:29s
Last reset time : 0h:0m:0s Last reset reason: Never
Error Subcode Sent : 0
Gr. Restart Time : 120 secs.
MAXIMUM Prefix : 4294967295 Send Community : Yes
Weight : 0 RtReflectorClient : No
Use MED : 0 Passive : No
AS-Override : No Allow-AS in : 0
Ignore Lead AS : No Out-Delay : 0
Remove Private AS : No Ttl : 1
Update Source :
Route-Map-In :
Route-Map-Out :
Password :
Capability : Announced Received
Route Refresh : No Yes
Dynamic : No No
Graceful Restart (ipv4-uni) Yes No
Multi-protocol (ipv4-uni) Yes Yes

Message Type Sent Received
------------------------------- --------- --------
Opens 1 1
Notifications 0 0
Capability 0 0
Updates 1 1
Keepalives 4 4
Route Refresh 0 0
Total 6 6

Prefix Activity Sent Received
------------------------------- --------- --------
Prefixes Current 1 3
Prefixes Total 1 3
Implicit Withdraw 0 0
Explicit Withdraw 0 0
Used as BestPath n/a 2

Local Policy Denied Prefixes Outbound Inbound
----------------------------------------------- ---- --------
Routemap 0 0
Bad lead AS n/a 0
Exceeded Max-prefix n/a 0
Exceeded Allow-as in n/a 0
Total 0 0

Number of NLRIs in the update sent 1 0

Synopsis:

show ip bgp as-path
Displays the list of AS_PATH that BGP has learnt from the routing information it has received.

HP Switch # show ip bgp as-path
BGP AS-Path Information

<table>
<thead>
<tr>
<th>AS Path</th>
<th>Metric</th>
<th>RefCount</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>?</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>200 i</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>300 ?</td>
<td>250</td>
<td>2</td>
</tr>
</tbody>
</table>

Synopsis:

show ip bgp redistribute
Displays the list of protocols whose routes are being redistributed into BGP.

HP Switch # show ip bgp redistribute

Route type RouteMap
-------------------------
static rtmap-static
rip

Synopsis:

show ip bgp summary
BGP solution use cases

Solution 1 — Campus iBGP

Two use cases are presented. The first illustrates the extension of BGP into an enterprise routing environment. The second case shows BGP connectivity in a remote site environments.

Figure 58 Solution 1 — Campus iBGP

Devices
A  WAN Gateway Router
B  Enterprise Core Router
C  Enterprise Core Router (Campus Edge)
D  Campus Core Routing Switch
E  Campus Distribution Routing Switch
F  Edge Switch

In the figure above, multiple campus domains are segmented by using BGP in the enterprise core. Traditionally, HP solutions have been used with devices E and F, facing the client or server network edges. With the introduction of BGP functionality, it becomes possible to position solutions at locations B, C, and D.

With proper filtering, a routing switch with 20,000 routes can be used in an iBGP deployment. A device at location C represents the boundary between interior gateway protocol (IGP) domains, and the BGP core. Functionality used on this device includes redistribution with route maps and the establishment of BGP communities. Devices at location B require AS path filtering. All locations
within the BGP AS require the remaining “Foundation” features (Route Reflection, Refresh, Multihop, etc.).

Additional Autonomous Systems may be configured within a network, resembling the enterprise core module as shown in the diagram. With larger enterprise customers, it is likely that an AS that is directly adjacent to IGP campus modules will be the location for HP foundation BGP solutions. See Figure 59 (page 347).

**Figure 59 Multiple internal AS deployment with Campus iBGP solution**

The core routing switch (device C) can establish eBGP peering with the Enterprise Core. It is possible to utilize the foundation Campus iBGP feature to satisfy some of these solutions.

A
Enterpriser Core Router

B
Enterprise Core Router (Campus Edge)

C
Campus Core Routing Switch

D
Campus Distribution Routing Switch (or Collapsed Core)

E
Edge Switch
Solution 2 — Remote site iBGP

A
Internet Gateway Router

B
Remote Site Core Routing Switch

C
Remote Site Distribution Routing Switch

D
Remote Site Edge Switches

You have the alternative of using static routes or BGP to connect to your service provider. For multi-homing or policy control, you can choose to deploy BGP. This may be used for internet connectivity. Foundation iBGP solutions do not carry full internet routing tables, so the diagram above requires that 1) only default routes are taken from the internet and 2) multiple VRF instances do not exist at a single physical remote site.

The deployment of device A may require additional traffic shaping and scalability features. If you prefer extending BGP routing to devices B or C, you can use BGP functionality on a routing switch. In this deployment model, the routing switch would be used for route redistribution and the marking of communities.

Troubleshooting BGP

Event log messages

1. Log per-peer established messages.
2. Log per-peer session-closed messages.
3. Log per-peer BGP notification messages.
4. Log graceful restart events.

Debug log messages

1. Log Per-Peer BGP State Transition.
2. Log per-peer arrivals of a new BGP update.
3. Log per-peer Time-outs (Hold-time, Graceful Restart Timeout).
4. Log Memory problems in case buffer-allocations fail.

No BGP peer relationship established

Symptom
Display BGP peer information using the `show ip bgp neighbor` command. The state of the connection to a peer cannot become established.

Analysis
To become BGP peers, any two routers need to establish a TCP session using port 179 and exchange open messages successfully.

Solution
1. Use the `show ip bgp neighbor` command to verify the peer’s IP address.
2. If the loopback interface is used, check whether the `neighbor connect interface` command is configured.
3. If the peer is a non-direct eBGP peer, check whether the `neighbor ebgp multihop` command is configured.
4. Check whether a route to the peer is available in the routing table.
5. Use the `ping` command to check connectivity.
6. Use the `display tcp status` command to check the TCP connection.
7. Check whether an ACL disabling TCP port 179 is configured.
<table>
<thead>
<tr>
<th><strong>Glossary</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ABR</strong></td>
</tr>
<tr>
<td><strong>ACE</strong></td>
</tr>
<tr>
<td><strong>ACL</strong></td>
</tr>
<tr>
<td><strong>active PoE port</strong></td>
</tr>
<tr>
<td><strong>active port</strong></td>
</tr>
<tr>
<td><strong>adjacent device</strong></td>
</tr>
<tr>
<td><strong>advertisement</strong></td>
</tr>
<tr>
<td><strong>all-traffic rate-limiting</strong></td>
</tr>
<tr>
<td><strong>AM</strong></td>
</tr>
<tr>
<td><strong>ARP</strong></td>
</tr>
<tr>
<td><strong>AS</strong></td>
</tr>
<tr>
<td><strong>ASBR</strong></td>
</tr>
<tr>
<td><strong>backbone area</strong></td>
</tr>
<tr>
<td><strong>backup</strong></td>
</tr>
<tr>
<td><strong>BDR</strong></td>
</tr>
<tr>
<td><strong>bps</strong></td>
</tr>
<tr>
<td><strong>BSD rcp</strong></td>
</tr>
<tr>
<td><strong>BSM</strong></td>
</tr>
<tr>
<td><strong>BSR</strong></td>
</tr>
<tr>
<td><strong>C-RP</strong></td>
</tr>
<tr>
<td><strong>CDP</strong></td>
</tr>
<tr>
<td><strong>chassis</strong></td>
</tr>
<tr>
<td><strong>CIDR</strong></td>
</tr>
<tr>
<td><strong>classifier-based mirroring policy</strong></td>
</tr>
<tr>
<td><strong>CoS</strong></td>
</tr>
</tbody>
</table>
DCA  Dynamic configuration arbiter. Determines the client-specific parameters that are assigned in an authentication session.

DD  Database description.

default route  A route defined as 0.0.0.0/0. OSPF uses type 3 (summary) defaults and type 7 (external) default routes.

destination  The host device that is connected to an exit port on the local source switch or a remote switch, and associated with a mirror-session number (1 to 4).

DHCP  Dynamic host configuration protocol.

DHCP relay  Allows you to extend the service range of your dhcp server beyond its single local network segment.

direction-based mirroring  On an interface configured for mirroring, the traffic direction (entering or leaving the switch or both) is used as criteria for selecting the traffic to be mirrored.

distance vector  A number representing distance.

DLC  Data link layer classification.

DLL  Data link layer.

DMA  Direct access memory. Transmits and receives packets between the CPU and the switch.

DNS  Domain name system.

domain suffix  Includes all labels to the right of the unique host name in a fully qualified domain name assigned to an IP address. For example, in the fully qualified domain name "device53.evergreen.trees.org," the domain suffix is "evergreen.trees.org," while "device53" is the unique (host) name assigned to a specific IP address.

DoS  Denial of service.

DR  Designated router. Used in networks having two or more routers and serves as the distribution point for forwarding updates throughout the network. Within a given VLAN or network, the router elected to forward a multicast flow from its IP source (in the VLAN or network) to the appropriate rendezvous point (either an RP or static-RP) in the PIM-SM domain.

DT  Distributed trunk.

DTD  Distributed trunking device.

DTE  Data terminal equipment.

DTIP  Distributed trunking internet protocol.

DTS  Distributed trunking switches.

dynamic RP  A PIM-SM router configured as a Candidate Rendezvous Point (C-RP).

ECMP  Equal cost multi-path (routing).

ECS  Emergency call service.

eedge router  Any router directly connected to a host or other endpoint in the network.

EEE  Energy efficient ethernet.

ELIN  Emergency location identification number. A valid telephone number in the North American Numbering Plan format and assigned to a multiline telephone system operator by the appropriate authority. This number calls a public service answering point (PSAP) and relays automatic location identification data to the PSAP.

exit port  The port to which a traffic analyzer or IDS is connected to receive mirrored traffic.

- For local mirroring, an exit port can be any port to which a traffic analyzer or IDS is connected and that is not configured as a monitored interface. You can configure up to four exit ports for local mirroring on a switch, using the command: mirror session port exit-port.

- For remote mirroring, the destination IP address (dst-ip) and exit port in a remote mirroring endpoint can belong to different VLANs. You can configure up to 32 exit ports for remote mirroring on a switch, using the command: mirror endpoint ip src-ip src-udp-port dst-ip exit-port.
exit switch
The switch with the exit port to which a destination device is connected. See also exit port.

external type-5 link-state advertisement
An LSA summarizing known external links for the backbone and normal areas.

external type-7 link state advertisement
An LSA originating with an ASBR in an NSSA and allowed only in the NSSA.

failed management module
A management module that did not pass self test and is not in standby mode.

FFI (event type)
Find, fix and inform. Event or alert log messages indicating a possible topology loop that causes excessive network activity and results in the network running slow.

FIB
Forwarding information base.

fixed or “well-known” traps
A switch automatically sends fixed traps (such as "coldStart", "warmStart", "linkDown", and "linkUp") to trap receivers using the public community name. These traps cannot be redirected to other communities. If you change or delete the default public community name, these traps are not sent.

flow
Multicast traffic having one source and one multicast group address (destination). This traffic may reach many hosts in different subnets, depending on which hosts have issued joins for the same multicast group. 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.

fully qualified domain name
The sequence of labels in a domain name identifying a specific host (host name) and the domain in which it exists. For example, if a device with an IP address of 10.10.10.101 has a host name of device53 and resides in the evergreen.trees.org domain, the device’s fully qualified domain name is device53.evergreen.trees.org and the DNS resolution of this name is 10.10.10.101.

GARP

GMB
GMB guaranteed minimum bandwidth. Provides a method for ensuring that each of a given port’s outbound traffic priority queues has a specified minimum consideration for sending traffic out on the link to another device. This can prevent a condition where applications generating lower-priority traffic in the network are frequently or continually “starved” by high volumes of higher-priority traffic.

GVRP
Garp vlan registration protocol. Manages dynamic 802.1Q VLAN operations, in which the switch creates temporary VLAN membership on a port to provide a link to another port in the same VLAN on another device.

host
A client device that requests multicast traffic by transmitting IGMP "joins"for a specific multicast group, such as a video conferencing application. Used in traffic mirroring to refer to a traffic analyzer or IDS.

host name
The unique, leftmost label in a domain name assigned to a specific IP address in a DNS server configuration. This enables the server to distinguish a device using that IP address from other devices in the same domain. For example, in the evergreen.trees.org domain, if an IPv4 address of 10.10.100.27 is assigned a host name of accounts015 and another IP address of 10.10.100.33 is assigned a host name of sales021, the switch configured with the domain suffix evergreen.trees.org and a DNS server that resolves addresses in that domain can use the host names to reach the devices with DNS-compatible commands.

ICMP
Internet control message protocol.

ICMP rate-limiting
Applies a rate-limit to all inbound ICMP traffic received on an interface, but does not limit other types of inbound traffic.

IDM
Identify-driven management.

IDS
Intrusion detection system.

IGMP
Internet group management protocol.

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.
IGP
Internet gateway protocol. A method for forwarding traffic between autonomous routing domains. Commonly used between OSPF and RIP domains.

IP addressing
Internet protocol (addressing). Configures the switch with an IP address and subnet mask to communicate on the network and support remote management access; configures multiple IP addresses on a VLAN; enables IP routing on the switch.

IRDP
ICMP router discovery protocol. Advertises the IP addresses of the routing interfaces on this switch to directly attached host systems.

ISC
Interswitch connect. A special interface that connects DTSs.

jumbo frame
An IP frame exceeding 1522 bytes in size. The maximum Jumbo frame size is 9220 bytes. (This size includes 4 bytes for the VLAN tag.)

jumbo VLAN
A VLAN configured to allow inbound jumbo traffic. All ports belonging to a jumbo and operating at 1 Gbps or higher can receive jumbo frames from external devices. If the switch is in a meshed domain, then all meshed ports (operating at 1 Gbps or higher) on the switch will accept jumbo traffic from other devices in the mesh.

KMS
Key management system.

LACP
Link aggregation control protocol.

link test
A test of the connection between the switch and a designated network device on the same LAN (or VLAN, if configured).

LLDP
Link layer discovery protocol. Provides a standards-based method for enabling the switches covered in this guide to advertise themselves to adjacent devices and to learn about adjacent LLDP devices.

LLDP neighbor
An LLDP device that is either directly connected to another LLDP device or connected to that device by another, non-LLDP layer 2 device (such as a hub). An 802.1D-compliant switch does not forward LLDP data packets even if it is not LLDP-aware.

LLDP-aware
A device that has LLDP in its operating code, regardless of whether LLDP is enabled or disabled.

LLDP-MED
LLDP-media-endpoint-discovery. LLDP-MED (ANSI/TIA-1057/D6) extends the LLDP (IEEE 802.1AB) industry standard to support advanced features on the network edge for Voice Over IP (VoIP) endpoint devices with specialized capabilities and LLDP-MED standards-based functionality.
Second definition: The TIA telecommunications standard produced by engineering subcommittee TR41.4, “VoIP Systems - IP Telephony infrastructure and Endpoints” to address needs related to deploying VoIP equipment in IEEE 802-based environments. This standard will be published as ANSI/TIA-1057.

LLDPDU
LLDP data unit. LLDP data unit LLDP data packet are transmitted on active links and include multiple TLVs containing global and per-port switch information. In this guide, LLDPDUs are termed "advertisements" or "packets".

local mirroring
The monitored (source) interface and exit port in a mirroring session are on the same switch.

local mirroring traffic destination
Port on the same switch as the source of the traffic being mirrored. See also remote mirroring traffic destination.

log throttle periods
Used to regulate (throttle) duplicate messages for recurring events.

LSA
Link-state advertisements. A message sent by a router to its neighbors to advertise the existence of a route to a destination known by the originating router.

LSDB
Link-state database.

master
The Owner or Backup router that is currently the physical forwarding agent for routed traffic using the VR as a gateway. There can be only one router operating as the Master for a network or (in the case of a multinetted VLAN) a subnet. If the router configured as the Owner for a VR is available to the network, it will also be the Master. If the Owner fails or loses availability to the network, the highest-priority Backup becomes the Master.

MED
Media endpoint. See LLDPMED.

MIB
Management information base. An internal database the switch maintains for configuration and performance information.

mini-GBICs
See GBICs.
MLD  Multicast listener discovery. IPv6 protocol used by a router to discover the presence of multicast listeners. MLD can also optimize IPv6 multicast traffic flow with the snooping feature.

MLTS  Multiline telephone system/service. A network-based and/or premises-based telephone system having a common interface with the public switched telephone system and having multiple telephone lines, common control units, multiple telephone sets, and control hardware and software.

mm  Management module.

monitored interface  The interface (port, VLAN, trunk, or mesh) on the source switch on which the inbound and/or outbound traffic to be mirrored originates, configured with one of the interface monitor or vlan monitor commands.

MPS  Maintenance power signature. The signal a PD sends to the switch to indicate that the PD is connected and requires power.

MRT  Multicast routing table.

MSTP  Multiple spanning tree protocol.

MTM  Multicast traffic manager. Controls and coordinates L3 multicast traffic for upper layer protocols.

MTU  Maximum transmission unit. The maximum size IP frame the switch can receive for Layer 2 frames inbound on a port.

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."

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.

multicast source  A single device originating multicast traffic for other devices (receivers).

NANP  North American numbering plan. A ten-digit telephone number format where the first three digits are an area code and the last seven-digits are a local telephone number.

Neighbor  See LLDP neighbor.

non-LLDP device  A device that is not capable of LLDP operation.

nonstop switching  The standby management module is synced continuously with the active management module so that all features and config files are the same on both management modules. The standby management module is ready to become the active management module. The transition is quick and seamless; switching continues without interruption.

normal area  Exists within an OSPF domain and connects to the backbone area through one or more ABRs (either physically or through a virtual link). Supports summary link-state advertisements and external link-state advertisements to and from the backbone area, as well as ASBRs.

NSSA  not-so-stubby-area. An OSPF area that limits advertisement of external and summary routes to the backbone area and allows controls on advertisements entering the area from the backbone.

offline management module  A management module that is offline because Management Module redundancy is disabled.

OOBM  Out-of-band management.

OSPF  Open short path first. A routing protocol that uses link-state advertisements (LSA) to update neighboring routers regarding its interfaces and information on those interfaces. Each routing switch maintains an identical database that describes its area topology to help a router determine the shortest path between it and any neighboring router.

oversubscribed  The state where there are more PDs requesting PoE power than can be accommodated.

oversubscribed queue  The condition where there is insufficient bandwidth allocated to a particular outbound priority queue for a given port. If additional, unused bandwidth is not available, the port delays or drops the excess traffic.

owner  The router configured in a VR to "own", the "virtual", Âµ IP address associated with the VR. (The virtual IP address for the VR must be configured as a real IP address on the VLAN on which the VR is configured. The Owner is automatically configured with the highest VRRP router priority in
the VR (255) and operates as the Master router for the VR unless it becomes unavailable to the


**PCM(+)** HP Switch Manager Plus. See PCM.

**PD** Powered device. An IEEE 802.3af-compliant or IEEE 802.3at-compliant device that receives its power through a direct connection to a 10/100Base-TX PoE RJ-45 port in an HP fixed-port or chassis-based switch. Examples of PDs include Voice-over-IP (VoIP) telephones, wireless access points, and remote video cameras.

**PIM** Protocol-independent multicast (routing). Enables IP multicast traffic to be transmitted for multimedia applications throughout a network without being blocked at routed interface (VLAN) boundaries.

**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.

**ping** Packet internet groper.

**ping test** A test of the path between the switch and another device on the same or another IP network that can respond to IP packets (ICMP Echo Requests).

**PLC** Physical layer classification.

**PMBRs** PIM border routers.

**PoE** Power over Ethernet. The method by which PDs receive power from a PoE module (operates according to the IEEE 802.3af standard).

**port-number priority** The type of power prioritization where, within a priority class, a PoE module assigns the highest priority to the lowest-numbered port in the module, the second-highest priority to the second lowest-numbered port in the module, and so on.

**primary image** The software version stored in primary flash on each management module.

**priority class** The type of power prioritization that uses Low (the default), High, and Critical priority assignments to determine which groups of ports will receive power.

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

**PSAP** Public safety answering point. Typically, emergency telephone facilities established as a first point to receive emergency (911) calls and to dispatch emergency response services such as police, fire and emergency medical services.

**PSCP** Putty SCP. See SCP.

**PSE** Powersourcing equipment. A PSE, such as a PoE module installed in a switch, provides power to IEEE 802.3af-compliant or IEEE 802.3at-compliant PDs directly connected to the ports on the module.

**QoS** Quality of service. Classifies and prioritizes traffic throughout a network, establishing an end-to-end traffic priority policy to manage available bandwidth and improve throughput of important data.

**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.

**RADIUS** Remote authentication dial-in user service.

**rapid switchover** Allows configuration of a timer (in seconds) for Layer 3 forwarding of packets. After failover, the route and neighbor entries in the forwarding information base (FIB) on the active management module are marked as stale. As new routes are added, the stale flag is reset. This continues for the number of seconds indicated by the timer, after which all remaining stale entries are removed.
remote mirroring

The monitored (source) interface and exit port in a mirroring session are on different switches. For remote mirroring, you must always configure the IP destination address and exit port (the remote mirroring endpoint) before you configure the monitored interface, by using the following commands:

On the remote (destination) switch:
mirror endpoint ip src-ip src-udp-port dst-ip exit-port

On the local (source) switch:
mirror session remote ip src-ip src-udp-port dst-ip

remote mirroring traffic destination

An HP switch configured to operate as the exit switch for mirrored traffic sessions originating on other HP switches. See also local mirroring traffic destination.

RFP

Reverse path forwarding. Uses a unicast routing table to find the path to the originator of the multicast traffic and sets up multicast "trees" for distributing multicast traffic.

RIP (interfaces)

Router information protocol.

RMON

Remote monitoring.

router

Any HP switch model covered by this guide and configured with IP routing enabled.

RP

Rendezvous point. A router that is either elected from a pool of eligible C-RPs (dynamic RPs) or statically configured (static RP) to support the distribution of traffic for one or more multicast groups and/or ranges of multicast groups. The RP for a given multicast group receives that group's traffic from a DR on the VLAN receiving the traffic from a multicast traffic source. The RP then forwards the traffic to downstream edge or intermediate PIM-SM routers in the path(s) to the requesting hosts (end points).

RP-set

A complete list of multicast-group-to-RP mappings the BSR has learned and distributed to the C-RPs in a given PIM-SM domain. The learned RP-set applies only to C-RPs, and not to static-RPs. (However, the show ip pim rp-set command lists both the learned RP-set from the BSR and any static-RPs configured on the router.)

RPF

Reverse path forwarding. A methodology that uses the unicast routing table created by IP protocols such as RIP and OSPF to determine the source address of a packet. PIM uses RPF to set up distribution trees for multicast traffic.

RPT

Rendezvous point tree. The path extending from the DR through any intermediate PIM-SM routers leading to the PIM-SM edge router(s) for the multicast receiver(s) requesting the traffic for a particular multicast group.

Rxmt QLen

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.

S/G

Source/group (pair). The unicast address of the server transmitting the multicast traffic and the multicast address to which the server is transmitting the traffic.

SA/DA

Source address/destination address.

SCP

Secure copy.

Secondary image

The software version stored in secondary flash on each management module.

selftest

A test performed at boot to ensure the management module is functioning correctly. If the module fails selftest, it does not go into active or standby mode. If both modules fail selftest, the switch does not boot.

sFlow

Flow sampling. An industry standard sampling technology, defined by RFC 3176, used to continuously monitor traffic flows on all ports providing network-wide visibility into the use of the network.

sFlow agent

A software process that runs as part of the network management software within a device. The agent packages data into datagrams that are forwarded to a central data collector.

sFlow destination

The central data collector that gathers datagrams from sFlow-enabled switch ports on the network. The data collector decodes the packet headers and other information to present detailed Layer 2 to Layer 7 usage statistics.

SM

Standby management module.
SNMP
Simple network management protocol. Allows you to manage the switch from a network management station, including support for security features, event reporting, flow sampling, and standard MIBs.

SNTP
Simple network time protocol. Synchronizes and ensures a uniform time among interoperating devices.

source (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.

source switch
The source switch on which the inbound and/or outbound traffic to be mirrored originates. See also Monitored Interface.

spoofed ping
An ICMP echo request packet intentionally generated with a valid source IP address and an invalid destination IP address. Spoofed pings are often created with the intent to oversubscribe network resources with traffic having invalid destinations.

SPT
Shortest path tree. The shortest path from the DR through any intermediate PIM-SM routers leading to the PIM-SM edge router(s) for the multicast receiver(s) requesting the traffic for a particular multicast group. Unless the RPT is in this path, it is excluded from the SPT.

SSH
Secure shell. Provides remote access to management functions on a switch via encrypted paths between the switch and management station clients capable of SSH operation.

SSL
Secure socket layer.

SSM
System support modules.

standard MTU
An IP frame of 1522 bytes in size. (This size includes 4 bytes for the VLAN tag.)

standby management module
A management module that is ready to become the active management module if the active management module fails.

static-RP
Static rendezvous point (S). A PIM-SM router manually configured as the distribution point for a multicast group or range of contiguous groups.

STFP
Secure FTP (file transfer protocol).

STP
Spanning tree protocol.

stub area
An OSPF area that does not allow an internal ASBR or external type-5 LSAs.

summary link-state advertisement
A type-3 LSA summarizing the available links within an OSPF area. This advertisement is sent by the ABR for an area to the backbone area for distribution to the other areas in the OSPF domain.

switchover
When the other management module becomes the active management module.

syslog
Debug/system logging feature.

TCP
Transmission control protocol. When the other management module becomes the active management module.

TFTP
Trivial file transfer protocol. When the other management module becomes the active management module.

threshold
A switch automatically sends all messages created when a system threshold is reached to the network management station that configured the threshold, regardless of the trap receiver configuration.

TLV
Type-length-value. A data unit that includes a data type field, a data unit length field (in bytes), and a field containing the actual data the unit is designed to carry (as an alphanumeric string, a bitmap, or a subgroup of information). Some TLVs include subelements that occur as separate data points in displays of information maintained by the switch for LLDP advertisements. (That is, some TLVs include multiple data points or subelements.)

topological database
See “link state database”

ToS
Type of service.

traffic mirroring
Intelligent mirroring.
trap receiver  Management station to which the switch sends SNMP traps and (optionally) event log messages sent from the switch. From the CLI you can configure up to ten SNMP trap receivers to receive SNMP traps from the switch.

trunk group  A set of up to eight ports configured as members of the same port trunk.

TTL  Time-to-live.

type-3 lsa, type-7 lsa  See "summary link-state advertisement."
See "external type-5 link state advertisement".
See "external type-7 link state advertisement".

UDLD  Uni-directional link detection. Monitors a link between two switches and blocks the ports on both ends of the link if the link fails at any point between the two devices.

UDP  See TCP.

virtual link  Used to provide connectivity from a normal area to the backbone when the subject area does not have an ABR physically linked to the backbone area.

VoIP  Voice over IP.

VR  Virtual router. Consists of one Owner router and one or more Backup routers, all of which belong to the same network or (in the case of a multinetted VLAN, the same subnet). The Owner is the router that owns the IP address(es) associated with the VR. The VR has one virtual IP address (or, in the case of a multinetted VLAN, multiple, virtual IP addresses) that corresponds to a real IP address on the Owner, and is assigned an identification number termed the VRID.

VRID  The identifier for a specific VR configured on a specific VLAN interface. On a given router, a VRID can be used for only one VR in a given VLAN, but can be used again for a different VR in a different VLAN.

VRRP  Virtual router redundancy protocol. Provides dynamic failover support as backup for gateway IP addresses (first-hop routers) so that if a VR’s Master router becomes unavailable, the traffic it supports will be transferred to a backup router without major delays or operator intervention, eliminating single-point-of-failure problems.

VT  Virus throttling.

warm reboot  Binary transfer feature that supports the download of software files from a PC or UNIX workstation.

warm standby  The active management module does not sync continuously with the standby management module. The standby management module boots to a certain point, syncs basic files, and only finishes booting if the active management module fails or you choose to change which module is the active management module. The transition is not seamless or immediate.

well-known address  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 predefined host groups.

Xmodem  Binary transfer feature that supports the download of software files from a PC or UNIX workstation.
Index

A
ABR
   definition, 200
   OSPF, 200
ACL
   operation with PIM, 62
   address
      IP, 126
   administrative distance, OSPF
      OSPF
         administrative distance, 210
   advertisement
      OSPF, 199
area
   OSPF, 179
   area information
      area, OSPF
         displaying area information, 179
      OSPF, 179
area range, OSPF
   configuring, 162, 210
area, OSPF
   assigning VLAN to, 157, 158
   configuring, 209
   definition, 202
ARP
   cache table, 121
   configuring parameters, 127
   enabling local proxy, 119
   how it works, 127
   local proxy option, 119
   proxy, 128
   assigning
      IP address, 126
      VLAN
   assigning OSPF area to, 157, 158
   authentication
      OSPF MDS, 170
   auto port setting, 27
   Autonomous system, OSPF
      OSPF autonomous system, 202
B
   blocked port
      from IGMP operation, 27
   boot
      with OSPF, 213
   BOOTP
      invalid gateway address, 242
   Bootp
      displaying configured gateway, 242
   broadcast forwarding, 249
   broadcast traffic
      enabling forwarding of directed, 129
   BSR
      change priority setting, 78
      configuration, 105
      display data, 96
      election, 105
      enable or disable operation, 77
      fault recovery, 106
      non-default settings, 97
      operation, 105
C
   C-RP
      add multicast group, 69, 81
      change hold time, 82
      configuring operation, 80
      defined, 350
      display config, 70, 99
      display status, 70, 99
      election priority, 82
      enabling or disabling, 81
      multicast groups, 80
      specify VLAN interface, 80
      with PIM-SM router, 350
   caches
      IP forwarding, 123
   Candidate Rendezvous Point see C-RP
   CIDR, 126
   circuit ID, 252
   configuration
      ARP parameters, 127
      default route, 133
      DHCP Relay, 240
      RIP, 136
      enabling RIP globally, 136
      router ID, 126
      static IP routes, 131
   configuring
      advertisement, 209
      OSPF
         assigning area range, 162, 210
   defaults
      OSPF, 212
      changing defaults, 166, 211
   Designated Router

359
defined, 351
election criteria, 105
in VLAN, 105

DHCP
assigning a gateway, 241
hop count, disabling, 243
hop count, displaying, 244
relay agent, 241

DHCP Relay, 249
broadcast
forwarding, 249
configuration, 240
enabling, 240
helper address, 242
hop count in requests, 249
minimum requirements, 249
Option 82
   circuit ID, 252
   packet forwarding, 249
   verifying configuration, 243
directed broadcasts, 129
displaying
   OSPF, 180
   restrict redistribution filters, display, 192
displaying information
   virtual link, 193
Downstream interface, 51
DR (designated router)
defined, 351
election criteria, 105
dynamic priority change, 292
   OSPF, 297
   RIP, 297

E
ECMP
   feature description, 205
   in OSPF, 205
defined, 351
election
   DR (designated router):OSPF election, 200
   enabling
      OSPF, 161
   enabling redistribution
      OSPF, 161
   event log
      counter, 63
   external LSA
      LSA, 180
defined, 351
electoral, displaying
   external LSA, 180

F
failover, VRRP, 293
filters
effect of IGMP, 37
   maximum allowed, 27
   flow, defined, 352
   forwarding
   directed broadcasts, 129
   parameters, IP routing
   configuring, 129
   forwarding port, IGMP, 27

G
gateway, DHCP, 241
glossary, 350
   graft
      max graft retries, 45
graft acknowledgement
      graft ack, 44

H
helper address for DHCP Relay, 242
hop count in DHCP requests
disabling, 243
displaying configuration, 244

I
IANA, 261
ICMP
   configuring, 129
   disabling messages, 129
IGMP
   benefits, 26
   effect on filters, 37
   Exclude Source, 28
   Fast Leave, 29
   high-priority disabled with PIM-, 62
   high-priority forwarding, 27
   Include Source, 28
   IP multicast address range, 37
   leave group, 28
   maximum address count, 27
   multicast group, 28
   multimedia, 26
   operation, 28
   port states, 27
   proxy
      forwarding, 33
      proxy: forward loop, 35
      proxy: forwarding commands, 24
      proxy: show command, 25
      proxy: vlan context command, 25
      query, 28
      report, 28
      status, 28
      traffic, 27
   Version 3, 28
IGMP control, 27
IP address
   assigning, 126
   CIDR notation, 126
   multiple, 292
   virtual, 285
IP forwarding cache, 123
IP interface parameters, 125
IP route exchange protocols, 123
IP route table; tables
  IP route, 122
IP routing
  ARP cache table, 121
  chain, 182
  changing ARP parameters, 127
  changing router ID, 126
  configuring static routes, 131
  default route, 133
  DHCP Relay configuration, 240
  directed broadcasts, 129
  forwarding cache, 123
  forwarding parameters, 129
  helper address, 242
  helper address, UDP, 126
  interface parameters, 125
IP static routes
  administrative distance, 132
  blackhole, 133
  configuration, 131
  default route, 125, 134
  default route, configuring, 133
  display, 132
  null interface, 134
  null route, 131
  VLAN state, 134
IP static routes:maximal, 120
overview, 120
parameter configuring; configuration: IP routing
  parameters, 126
Proxy ARP, enabling, 128
redistribution, 225
route exchange protocols, 123
route policy, 215
  configuring, 224
  match commands, 225
  prefix lists, 215
  route maps, 224
  set commands, 222
router ID, 201
router ID; OSPF: router ID, 200
routining table, 122
static route configuration, 131
static route parameters, 134
static route types, 133
static routes
  discard traffic, 131
  discard, ICMP notification, 131
tables and caches, 121
type-7 LSA, 352
VLAN interface; VLAN interface: description, 121
IRDP
  configuring;, 237
  displaying information, 239
  enabling globally, 237
  enabling on VLAN interface;, 238
L
loopback interface
router priority; IP routing
  loopback interface, 201
LSA
  displaying information, 180
  LSA
    displaying, 185
M
management VLAN, 245
match commands, 225
MDS
  MDS authentication
    OSPF, 170
metric type
  metric
    OSPF redistribution, 162
  multicast source, defined, 354
multinetted VLANS and Option 82, 257
multiple relay agents, 254
N
near failovers
  statistic, 283
  VRRP, 281
O
Option 82, 250
  circuit ID, 252
  compliance, 250
  configuring operation, 245
  field content, 245
  forwarding policy, 253
  management VLAN, 245, 252
  multinetted VLANS, 257
  multiple relay agents, 254
  operation, 251
  Option 82 field, 250
  overview, 250
  Relay Agent Information, 250
  remote ID, 252
  requirements, 251
  server support, 251
  validating server response packets, 255
originator router, 50
OSPF
  ABR, 358
  ABR, connection requirement, 210
  ABR, range configuration, 208
  administrative distance, 208, 210
  administrative distance; OSPF: route choice, influencing, 165
  advertisement, blocking, 164
  area, 157, 158, 202, 208, 209, 354
  area border router; OSPF: ABR, 200
  area configuration, 209
  area range, 162, 210
  area types, 202
  ASBR, 200, 208
  ASBR, advertising, 205
ASBR, in NSSA, 208
authentication, 170, 174, 208, 212
description, 169, 211, 212
interface, 211
MD5, 170, 175
password, 169, 174
authentication:MD5, 150, 151, 170
authentication:password, 150, 151
autonomous system boundary router, 200
backbone area, 202, 350
backbone area, configure;OSPF:normal area, configure, 154
backbone area:, 202
blocking routes, 210
boot, 213
chain
chain, key management, 182
changing compliance setting, 153
changing port parameters, 153
configuration rules, 208
configuration steps, 152
cost, 208
cost; OSPF: summary cost, 163
dead-interval, 208
default parameter settings, 208
default port parameters, 153
default route, 351
displaying configuration and status, 177
displaying information, 177, 179, 180, 182, 185, 193
neighbor, 190
virtual link, 193
displaying redistribution, 191
DR (designated router), 200
enabling, 153, 207
equal cost multi-path (ECMP) multiple next-hop routing, 205
external LSA, 352
external route cost options, 156
external routes, redistribution, 208
general configuration steps, 208
general information, 177
hello-interval, 208
interface, 166, 211
interface parameters, 166
interior router, 199
link-state advertisement, 352
loopback interface, 201, 208
loopback interface, assigning, 158
loopback interface, redistribution, 159
LSA, 352
LSA types, 199
LSA, external, reduction, 205
MD5 authentication, 170
neighbor, 211
no-summary, 156
no-summary, effect, 205
normal area, 202, 203, 354
NSSA, 199, 202, 203
NSSA, configuring, 155
overview, 152
parameters, 212
passive, 175, 212
password, 169
priority, 208
range, blocking, 165
redistribution, 161, 162
metric, 161
redistribution filters, 192
redistribution, configuring, 160
redistribution, loopback interface, 159
reload, 213
restrict redistribution., 210
RFC 1583 compliance option, 208
RFC 1583, compliance setting, 209
RFC 1583, example, 154
RFC 2178, 209
RFC 2328, 199, 204, 209
RFC 2328;RFCs:RFC 2328, 204
RFC 3101, 199
RFC 3101;RFCs:RFC 3101, 204
RFC compliance, 204
route choice, influencing, 210
router ID, 126, 186, 187, 190, 193, 196, 201, 204, 205, 207, 212
router ID, displayed, 179, 180, 181
routing table, displaying
routing table, displaying, 195
show commands, 177
show passive information, 176
software license requirements, 121
SPF statistics, displaying, 194
stub area, 202, 203, 357
stub area, configuring, 155
summarizing routes, 210
summary link-state-advertisement, 357
topological database, 357
transit area, 211
transit area ID, 172, 173, 174
traps, 165, 208
type-3 default summary LSA, 156
type-3 LSA, 204, 358
type-3 summary LSA, 156, 205
type-5 LSA, 352
type-7 default external LSA, 156, 205
type-7 external LSA, 204, 358
type-7 summary LSA, 156, 205
virtual link, 193, 210, 212, 358
configuration, 211
interface parameters, 212
virtual neighbor:displaying information;virtual neighbor:OSPF:displaying information;OSPF:displaying information;virtual neighbor, 192
VLAN/subnet statistics, displaying, 183
with Pre-empt Delay Timer, 294
P
parameters
IP interface, 125
OSPF interface, 166
virtual link, 212
peers, RIP
displaying information, 144
PIM hello message
   hello delay, 44
PIM interfaces
   VLAN, 49
PIM-DM
   Asset Timer, 51
   bandwidth conservation;PIM-DM:state refresh, 61
   common subnet requirement;PIM-DM:subnet, common,
      60
   configuration, 40, 48, 61
   configuration order, recommended, 61
   configuration, general elements, 61
   configuration, router;PIM-DM:router configuration, 61
   default settings recommended, 61
draft versions 1 and 2;PIM-DM:compatible draft
   versions, 58
   error messages, 63
   expire time, 52, 53
   extended branch;PIM-DM:pruned branch, 59
flood and prune, 59, 60
flood and prune cycle, 62
flow, bridged, 63
flow, equalizing, 64, 65, 66
flow, multicast, limit, 64
flow, software, 41
flow;PIM-DM:flood;PIM-DM:prune;PIM-DM:join, 59
   forwarding, 51
general operation, 58
graft packets, 38, 44
   hello interval, effect, 43
   IGMP requirement, 62
   IGMP version 1;PIM-DM:IGMP version 2;PIM-DM:IGMP
      version 3;, 58
   IGMP, per VLAN, 59
interfaces, 53
IP address required, 62, 64
join, 59, 352
log message, 63
log message counter operation, 63
log message;, 63
   Metric, 51
   Metric Pref, 51
   MIB support, 58
MRT, 63
MRT;PIM-DM:flow, hardware, 41
multicast address, 59, 354, 356
multicast router, Asset Timer, 56
multicast router, multiple, 55
multicast routing, defined, 354
multicast server, 356
multinetted VLAN, 46
multinetted VLAN:common subnet required, 43
neighbor, PIM, 39, 49, 56, 355
prune, 51, 56
prune delay, 38, 45
prune reason, 56
prune state;PIM-DM:forwarding state, 60
   prune-pending state, 46
   pruning;, 60
RFC 2932 exceptions;RFCs:RFC 2932 MIB exceptions,
   66
RFCs, applicable;RFCs:PIM-applicable, 66
RIP;PIM-DM:OSPF;PIM-DM:static route, 59
route data, 48
routing protocol, 61
routing switch 9300, 62
RP Tree, 51
S/G pair, 356
SNMP traps, 40
software license requirements, 39
source address, unicast, 356
state refresh, 38, 40, 42, 55, 57, 62
state refresh, on other routers, 62
state refresh;, 60
time-to-live threshold, 39, 46
traps, SNMP, 40
tree, multicast, 59
TTL zero, 63
unicast routing, 58, 59
unicast source address, server, 356
up time, 52, 53
version differences, 65
VLAN support, outbound;PIM-DM:VLAN support,
   inbound, 58
VLAN, flow limit;PIM-DM:flow, VLAN limit, 58
VLAN, multinetted;PIM-DM:multinetted VLAN, 60
XRRP, 58
PIM-SM
border routers, 104
BSR, 104, 105
   message interval, 69, 79
   non-default settings, 97
   priority setting, 78
   protocol, 101
changing DR priority, 68, 76
compatible draft versions, 102
configuration, 94
configuring C-RPs, 79
Designated Router, 104
display BSR data, 96
display C-RP config, 70, 99
display config, 92
display status, 92
DR, 351
   priority, 95
draft versions 1 and 2, 102
enable/disable SNMP Traps, 82
entries in routing table, 70, 93
event log messages, 113
expire time, 94
features, 101
flow capacity, 101
flow, defined, 352
flow, software, 82
flow, VLAN limit, 101
group address, 70, 87, 93
hello delay, 75
hello hold-time, 74
hello interval, 75
hello interval, effect, 75
IGMP link, 101
IGMP version 1, 102
IGMP version 2, 102
IGMP version 3, 102
join, 352
join/prune interval, 69, 83
lan-prune-delay, 75
list interfaces, 93
MIB support, 102
MRT, 70, 93
multicast group distribution, 69, 78
multicast source, 354
neighbor, 87
neighbor, PIM, 70, 94
non-flooding model, 102
operating notes, 100
PMBR not supported, 104
propagation delay, 75
prune, 90
delay, 68, 75
prune delay, 68, 76
prune-pending state, 76
rendezvous point, 356
rendezvous point tree, 356
router types, 104
RP, 104
RP mapping, 101
RP-Set command, 356
RPF, 356
shortest path tree, 357
show VLAN configs, 93
SNMP traps, 92
software license requirements, 101
source address, 70, 87, 93
state refresh, 92, 94
static rendezvous point, 357
static RP, 104
traps, SNMP, 92
unicast routing, 101
using SPT controls, 83
VLAN support, inbound, 101
VLAN support, outbound, 101
VLAN, flow limit, 101
VRRP, 102
ping
VRRP backup responds to, 289
PMBR, 104
port
auto, IGMP, 27
blocked, IGMP, 27
forwarding, IGMP, 27
state, 27
Pre-empt DelayTimer
backward compatibility, 295
PDT value, 295
with older devices, 294
Pre-empt DelayTimer, 270
prefix lists, 215
Premium License
OSPF, 121
PIM-DM, 58
PIM-SM, 101
VRRP, 284
priority
IP multicast traffic, 27
protocols
IP route exchange, 123
Proxy ARP, enabling, 128
proxy forwarding, IGMP, 34
R
redistribution, 140, 225
and route policy, 161
OSPF
redistribution information, 191
reload
with OSPF, 213
Rendezvous Point Tree, defined, 356
Rendezvous Point, defined, 356
Reverse Path Forwarding, defined, 356
RFCs
RFC 1583 compliance option, 208, 209
RFC 2178, 204, 209
RFC 2328, 199, 204, 209
RFC 2338, 296
RFC 2787, 296
RFC 3101, 199
RFC 3768, 287, 288, 296
RFC 3768;, 289
RFC 4061, 102
RIP
changing cost of RIP routes, 139
changing RIP type, 138
changing the RIP metric, 139
configuring, 136
configuring an authentication key, 138
displaying configuration and status, 141
displaying general information, 141
displaying information, 141
displaying interface information, 143
displaying peer information, 144
displaying redistribution information, 145
displaying restrict information, 145
enabling globally, 136
enabling on a VLAN, 138
enabling on the routing switch, 137
enabling route redistribution, 140
entering RIP router context, 137
general information, 141
global parameters, 146
interface information, 143
interface parameters, 146
parameters and defaults, 146
peer information, 144
redistribution, 140
and route policy, 140
displaying, 145
enabling, 140
redistribution filters
displaying, 145
redistribution into RIP, 147
redistribution, configuring, 147
restrict filter information, 145
restrict redistribution, 145
route maps, 224
route policy, 215
configuring, 224
router ID, changing, 126
router, multicast, with IGMP, 27
RP
defined, 356
RP-Set, defined, 356
RPF, defined, 356
RPT
traffic restricted to, 104
S
set commands, 222
Shortest Path Tree, defined, 357
SPF
counting scheduling, 176
SPF algorithm
displaying OSPF statistics, 194
SPT
defined, 357
operation, 103
PIM-SM traffic, 83
static IP routes, 133
configuring, 131
route types, 133
Static Rendezvous Point see See static-RP
static RP
manual configuration, 83
static-RP
defined, 357
subnet, 28
T
tables
ARP cache, 121
IP, 121
tracked entities
displaying, 271
transit area
OSPF, 211
traps
OSPF, 165
U
UDP broadcast forwarding, 258
address types, 262
application, 261
configure, 258
global enable, 258
invalid entry, 262
IP helper address, effect, 261
maximum entries, 261
port-number ranges, 261
subnet address, 262
subnet masking, 262
UDP/TCP port number listing, 261
unicast address, 262
VLAN, subnetted, 262
unicast routing protocol
RIP, connected, OSPF, static route, other, 51
V
virtual link
authentication, 174, 212
change settings, 212
OSPF, 174, 212
virtual MAC address, 288
VLAN
IGMP configuration;IGMP:configure per VLAN, 16
interface, 49
VLAN interface
IP routing parameters, 125
OSPF
interface parameters, 166
VR
interface parameters, 166
VR
advertisement interval, 289
changes, 289
deactivate, 289
defined, 358
IP address, 289
IP address limit, 296
IP address, delete, 296
MAC address, 285
MAC address, source, 285
maximum in a VLAN, 286
maximum per switch, 289
maximum per VLAN, 289
membership, 286
multiple IP addresses, 292
multiple VRs in VLAN, 286
multiple, in a VLAN, 287
operation, 286
specific, 278
subnet limit per VLAN, 296
VRID
configure, 263, 266
defined, 358
maximum per VLAN, 263, 266
VRPP, 263, 266, 285, 286, 287, 289, 292, 296, 358
advantages, 265
advertisement, 286
function, 287
interval, 287, 289
ARP response, 286, 288
authentication type, 296
backup responds to ping, 289
Backup router, 264, 288
  as Master, 264
defined, 350
elected as Master, 287
  multiple, 285
no response to ping, 289
not receiving advertisements, 296
precedence, 350
priority, 288
  priority, configure, 268
  virtual IP address, 288
backup, configuring, 263, 266
configuration example, 292
debug, 284
disable global, 263, 265
disable on VR, 269
disabled during configuration, 263, 266
disabling operation, 270
display, 278
  statistics, global, 264, 279
  uptime, 280
  VR, specific, 264
displaying tracked entities, 271
dropped packets, 296
dynamic priority change, 292
election process, 284
enable global, 263, 265
enable on VR, 269
event log, 263, 265
event log messages, 297
example, 285, 291
failback, 264, 284, 286
failover, 264, 285, 286, 288
failover operation, 293
failover, VRRP, 264
global configuration, 277
IP address, deleting, 289
IP address, per VR, 289
IP address, real, 285, 287
IP address, virtual, 285, 286, 287, 288
IPv4, 296
LACP and tracked ports, 297
MAC address
  shared, 286
  source, 286, 288
  virtual, 288
Master router, 264, 284, 287
see also Owner router
  advertisements failing, 296
election, 287
  Owner unavailable, 287
Master router: defined, 353
multinetted VLAN, 286, 287, 289
near failovers, 283
near failovers stat, 281
overview, 264
Owner priority see priority
Owner priority, 255, 289
Owner router, 264, 284, 287
see also Master router
default Master, 287
defined, 354
priority, 287
owner, configuring, 263, 266
pre-empt delay time, 270
pre-empt delay timer and OSPF, 294
Pre-empt Delay Timer with LACP, 294
Pre-empt Delay Timer with older devices, 294
Pre-empt Delay Timer, backward compatibility, 295
Pre-empt Delay Timer, PDT value, 295
pre-empt mode, 288
pre-empt mode, configure, 263, 269
preempt mode, enabled, 269
preempt-delay time, 0 seconds, 276
primary-ip-address, lowest, 269
priority, 285, 287
  Backup, 286, 289, 290
  Backup default, 287
  Owner, 284, 286, 287, 289, 290
  Owner default, 288
  range for Backup router, 287
VR, 288
priority, Owner, 284, 286, 287, 289, 290
real gateway, 287
RFC see RFCs
router vrrp traps, enabled, 265
router vrrp, disabled, 265
software license requirements, 284
source address for VR, 285
standards compliance, 296
traps, disable, 263, 265
traps, enable, 263, 265
virtual router see VR
  virtual router ID see VRID
VLAN, subnetted, 287
VR
  advertisement interval, change;, 268
  virtual IP address, configure, 269
  virtual IP address, default, 269
VR instance, disabled, 267
VR priority see VRRP, priority
VR priority, 100, 286
VRID, 285, 286, 288