This document is protected by copyright. Except as specifically permitted herein, no portion of the provided information can be reproduced in any form, or by any means, without prior written permission from Alcatel-Lucent. Alcatel, Lucent, Alcatel-Lucent and the Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.

Copyright © 2011 Alcatel-Lucent. All rights reserved.
# TABLE OF CONTENTS

## Preface

| Preface | 15 |

## Getting Started

| Alcatel-Lucent 7450 ESS-Series Router Configuration Process | 19 |

## Multicast

<table>
<thead>
<tr>
<th>Introduction to Multicast</th>
<th>22</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast Models</td>
<td>23</td>
</tr>
<tr>
<td>Any-Source Multicast (ASM)</td>
<td>23</td>
</tr>
<tr>
<td>Source Specific Multicast (SSM)</td>
<td>23</td>
</tr>
<tr>
<td>IPv6 Multicast</td>
<td>25</td>
</tr>
<tr>
<td>Multicast Listener Discovery (MLD v1 and v2)</td>
<td>25</td>
</tr>
<tr>
<td>PIM SSM</td>
<td>25</td>
</tr>
<tr>
<td>IPv6 PIM ASM</td>
<td>26</td>
</tr>
<tr>
<td>Embedded RP</td>
<td>26</td>
</tr>
</tbody>
</table>

## Core Router Multicast Requirements

<table>
<thead>
<tr>
<th>Internet Group Management Protocol</th>
<th>27</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Versions and Interoperability Requirements</td>
<td>28</td>
</tr>
<tr>
<td>IGMP Version Transition</td>
<td>28</td>
</tr>
<tr>
<td>Source-Specific Multicast Groups</td>
<td>29</td>
</tr>
<tr>
<td>Protocol Independent Multicast Sparse Mode (PIM-SM)</td>
<td>30</td>
</tr>
<tr>
<td>PIM-SM Functions</td>
<td>30</td>
</tr>
<tr>
<td>Encapsulating Data Packets in the Register Tunnel</td>
<td>33</td>
</tr>
<tr>
<td>PIM Bootstrap Router Mechanism</td>
<td>33</td>
</tr>
<tr>
<td>PIM-SM Routing Policies</td>
<td>33</td>
</tr>
<tr>
<td>Reverse Path Forwarding Checks</td>
<td>35</td>
</tr>
<tr>
<td>Anycast RP for PIM-SM</td>
<td>36</td>
</tr>
</tbody>
</table>

## Multicast Extensions to MBGP

| MBGP Multicast Topology Support | 39 |

## Multicast Source Discovery Protocol (MSDP)

<table>
<thead>
<tr>
<th>MBGP Multicast Topology Support</th>
<th>39</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anycast RP for MSDP</td>
<td>40</td>
</tr>
<tr>
<td>MSDP Procedure</td>
<td>41</td>
</tr>
<tr>
<td>MSDP Peer Groups</td>
<td>42</td>
</tr>
<tr>
<td>MSDP Mesh Groups</td>
<td>42</td>
</tr>
<tr>
<td>MSDP Routing Policies</td>
<td>43</td>
</tr>
<tr>
<td>Multicast in Virtual Private Networks</td>
<td>44</td>
</tr>
</tbody>
</table>

## Multicast Debugging Tools

<table>
<thead>
<tr>
<th>Multicast Connection Admission Control (MCAC)</th>
<th>48</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mtrace</td>
<td>48</td>
</tr>
<tr>
<td>Mstat</td>
<td>47</td>
</tr>
<tr>
<td>Mrinfo</td>
<td>47</td>
</tr>
<tr>
<td>Multicast Source Discovery Protocol (MSDP)</td>
<td>48</td>
</tr>
<tr>
<td>BTV</td>
<td>48</td>
</tr>
<tr>
<td>Interface-Level CAC</td>
<td>52</td>
</tr>
<tr>
<td>Bundle-Level CAC</td>
<td>52</td>
</tr>
<tr>
<td>Dealing with Configuration Changes</td>
<td>53</td>
</tr>
</tbody>
</table>
## Table of Contents

LAG Interworking ................................................................. 54  
CAC Policy for Split Horizon Groups ........................................ 55
Multicast Configuration Process Overview ................................. 56
Configuration Notes ............................................................... 57
  General .............................................................................. 57
Configuring Multicast Parameters with CLI ................................. 59
Multicast Configuration Overview ............................................. 60
Basic Configuration ............................................................... 61
Common Configuration Tasks .................................................. 64
  Configuring IGMP Parameters ............................................. 64
  Enabling IGMP ................................................................. 64
  Configuring an IGMP Interface ............................................. 65
  Configuring Static Parameters ............................................. 66
  Configuring SSM Translation ............................................... 68
Configuring PIM Parameters .................................................. 69
  Enabling PIM ................................................................ 69
  Configuring PIM Interface Parameters .................................. 70
  Importing PIM Join/Register Policies ..................................... 75
Configuring Multicast Source Discovery Protocol (MSDP) Parameters ............................................. 77
Configuring MCAC Parameters ............................................... 78
Service Management Tasks .................................................... 81
Disabling IGMP or PIM ......................................................... 81
Multicast Command Reference ............................................... 85
Configuration Commands ....................................................... 99
  Generic Commands ......................................................... 99
  Multicast Commands ....................................................... 100
  Router IGMP Commands .................................................. 103
  Router PIM Commands .................................................... 113
  Multicast CAC Policy Configuration Commands ................. 140
MLD Commands .................................................................. 148
Operational Commands ......................................................... 155
Show Commands ................................................................. 161
  IGMP Commands ............................................................ 161
  Show Router PIM Commands ............................................. 174
Clear Commands ................................................................ 214
Debug Commands .............................................................. 222
  Debug IGMP Commands .................................................. 222
  Debug PIM Commands .................................................... 225

## RIP

RIP Overview ................................................................. 232
  RIP Features ............................................................... 233
  RIP Version Types ....................................................... 233
  RIPv2 Authentication ..................................................... 233
  Metrics ......................................................................... 234
  Timers ......................................................................... 234
  Import and Export Policies ............................................. 234
  RIP Packet Format ....................................................... 235
  Hierarchical Levels ....................................................... 237
# Table of Contents

RIP Configuration Process Overview ................................................................. 238  
Configuration Notes ............................................................................................ 239  
  General ............................................................................................................... 239  
  Configuring RIP with CLI .................................................................................. 241  
RIP Configuration Overview ................................................................................. 242  
  Preconfiguration Requirements ......................................................................... 242  
  RIP Hierarchy .................................................................................................... 242  
Basic RIP Configuration ......................................................................................... 243  
Common Configuration Tasks ................................................................................ 244  
  Configuring Interfaces ....................................................................................... 245  
  Configuring a Route Policy ................................................................................ 246  
  Configuring RIP Parameters ............................................................................. 248  
  Configuring Global-Level Parameters ............................................................... 250  
  Configuring Group-Level Parameters ............................................................... 251  
  Configuring Neighbor-Level Parameters ......................................................... 252  
RIP Configuration Management Tasks ................................................................. 253  
  Modifying RIP Parameters ................................................................................ 253  
  Deleting a Group ............................................................................................... 254  
  Deleting a Neighbor .......................................................................................... 254  
RIP Command Reference ....................................................................................... 255  
  RIP Configuration Commands ......................................................................... 259  
     Generic Commands ......................................................................................... 259  
     RIP Commands .............................................................................................. 261  
  Show Commands ............................................................................................... 271  
  Clear Commands ............................................................................................... 282  
  Debug RIP Commands ....................................................................................... 283  

**OSPF**

Configuring OSPF ................................................................................................. 286  
OSPF Areas ........................................................................................................... 287  
  Backbone Area .................................................................................................. 287  
  Stub Area ........................................................................................................... 288  
  Not-So-Stubby Area ......................................................................................... 289  
  OSPFv3 Graceful Restart Helper ..................................................................... 295  
Virtual Links .......................................................................................................... 296  
Neighbors and Adjacencies ................................................................................... 297  
Link-State Advertisements .................................................................................... 298  
Metrics .................................................................................................................. 298  
Authentication ....................................................................................................... 299  
IP Subnets ............................................................................................................. 300  
Preconfiguration Recommendations ...................................................................... 300  
Multiple OSPF Instances ..................................................................................... 301  
  Route Export Policies for OSPF ...................................................................... 301  
  Preventing Route Redistribution Loops ............................................................ 302  
IP Fast-reroute (IP FRR) For OSPF and IS-IS Prefixes ........................................ 303  
  IP FRR Configuration ....................................................................................... 303  
  ECMP Considerations ....................................................................................... 304  
  IP FRR and RSVP Shortcut (IGP Shortcut) ...................................................... 305  
  IP FRR and BGP Next-Hop Resolution ............................................................ 305
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OSPF and IS-IS Support for Loop-Free Alternate Calculation</strong></td>
<td>305</td>
</tr>
<tr>
<td><strong>OSPF Configuration Process Overview</strong></td>
<td>311</td>
</tr>
<tr>
<td><strong>Configuration Notes</strong></td>
<td>312</td>
</tr>
<tr>
<td><strong>General</strong></td>
<td>312</td>
</tr>
<tr>
<td><strong>OSPF Defaults</strong></td>
<td>312</td>
</tr>
<tr>
<td><strong>Configuring OSPF with CLI</strong></td>
<td>313</td>
</tr>
<tr>
<td><strong>OSPF Configuration Guidelines</strong></td>
<td>314</td>
</tr>
<tr>
<td><strong>Basic OSPF Configuration</strong></td>
<td>315</td>
</tr>
<tr>
<td><strong>Configuring the Router ID</strong></td>
<td>316</td>
</tr>
<tr>
<td><strong>Configuring OSPF Components</strong></td>
<td>317</td>
</tr>
<tr>
<td><strong>Configuring OSPF Parameters</strong></td>
<td>317</td>
</tr>
<tr>
<td><strong>Configuring an OSPF Area</strong></td>
<td>318</td>
</tr>
<tr>
<td><strong>Configuring a Stub Area</strong></td>
<td>319</td>
</tr>
<tr>
<td><strong>Configuring a Not-So-Stubby Area</strong></td>
<td>320</td>
</tr>
<tr>
<td><strong>Configuring a Virtual Link</strong></td>
<td>321</td>
</tr>
<tr>
<td><strong>Configuring an Interface</strong></td>
<td>323</td>
</tr>
<tr>
<td><strong>Configuring Authentication</strong></td>
<td>325</td>
</tr>
<tr>
<td><strong>Assigning a Designated Router</strong></td>
<td>328</td>
</tr>
<tr>
<td><strong>Configuring Route Summaries</strong></td>
<td>330</td>
</tr>
<tr>
<td><strong>Configuring Route Preferences</strong></td>
<td>332</td>
</tr>
<tr>
<td><strong>OSPF Configuration Management Tasks</strong></td>
<td>334</td>
</tr>
<tr>
<td><strong>Modifying a Router ID</strong></td>
<td>334</td>
</tr>
<tr>
<td><strong>Deleting a Router ID</strong></td>
<td>336</td>
</tr>
<tr>
<td><strong>Modifying OSPF Parameters</strong></td>
<td>337</td>
</tr>
<tr>
<td><strong>OSPF Command Reference</strong></td>
<td>339</td>
</tr>
<tr>
<td><strong>Configuration Commands</strong></td>
<td>345</td>
</tr>
<tr>
<td><strong>Generic Commands</strong></td>
<td>345</td>
</tr>
<tr>
<td><strong>OSPF Global Commands</strong></td>
<td>346</td>
</tr>
<tr>
<td><strong>OSPF Area Commands</strong></td>
<td>363</td>
</tr>
<tr>
<td><strong>Interface/Virtual Link Commands</strong></td>
<td>368</td>
</tr>
<tr>
<td><strong>Show Commands</strong></td>
<td>379</td>
</tr>
<tr>
<td><strong>Clear Commands</strong></td>
<td>423</td>
</tr>
<tr>
<td><strong>OSPF Debug Commands</strong></td>
<td>425</td>
</tr>
</tbody>
</table>

**IS-IS**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring IS-IS</strong></td>
<td>432</td>
</tr>
<tr>
<td><strong>Routing</strong></td>
<td>433</td>
</tr>
<tr>
<td><strong>IS-IS Frequently Used Terms</strong></td>
<td>435</td>
</tr>
<tr>
<td><strong>ISO Network Addressing</strong></td>
<td>436</td>
</tr>
<tr>
<td><strong>IS-IS Unnumbered Interfaces</strong></td>
<td>438</td>
</tr>
<tr>
<td><strong>IS-IS PDU Configuration</strong></td>
<td>439</td>
</tr>
<tr>
<td><strong>IS-IS Operations</strong></td>
<td>439</td>
</tr>
<tr>
<td><strong>IS-IS Route Summarization</strong></td>
<td>440</td>
</tr>
<tr>
<td><strong>IS-IS Administrative Tags</strong></td>
<td>441</td>
</tr>
<tr>
<td><strong>Setting Route Tags</strong></td>
<td>441</td>
</tr>
<tr>
<td><strong>Using Route Tags</strong></td>
<td>442</td>
</tr>
<tr>
<td><strong>IS-IS Configuration Process Overview</strong></td>
<td>443</td>
</tr>
<tr>
<td><strong>Configuration Notes</strong></td>
<td>444</td>
</tr>
<tr>
<td><strong>General</strong></td>
<td>444</td>
</tr>
</tbody>
</table>
## Table of Contents

**BGP**

- **BGP Overview** .................................................. 542
- **BGP Communication** ............................................ 542
  - **Message Types** ................................................ 542
- **Group Configuration and Peers** ................................ 544
- **Hierarchical Levels** ............................................. 545
- **Route Reflection** ................................................. 545
- **Fast External Failover** ........................................... 548
- **Sending of BGP Communities** ................................... 548
- **BGP Route Tunnel** ................................................ 549
  - **ECMP and BGP Route Tunnels** ................................ 549
  - **Layer 2 Services and BGP Route Tunnel** ..................... 549
  - **BGP Route Tunnel SDP Binding** ................................ 549
  - **BGP Route Tunnel Based BGP-AD Support** ..................... 550
  - **BGP Route Tunnel with multi-hop eBGP session** ............. 550
  - **RSVP-TE LSP Shortcut for BGP Next-Hop Resolution** ........ 551
  - **Core IPv4 Prefix Resolution** ................................ 551
  - **Handling of Control Packets** ................................ 552
  - **BGP Confederations** ............................................ 553

**IS-IS**

- **IS-IS Configuration Overview** .................................. 445
  - **Modifying Global IS-IS Parameters** ........................... 462
  - **Modifying IS-IS Interface Parameters** ....................... 463
  - **Configuring IS-IS Interface Parameters** ....................... 452
  - **Configuring IS-IS Components** ................................ 452
  - **Enabling IS-IS** ................................................ 452
  - **Disabling IS-IS** ............................................... 461
  - **Removing IS-IS** ............................................... 461
  - **Modifying Router-Level Parameters** .......................... 452
  - **Configuring ISO Area Addresses** ................................ 454
  - **Configuring Global IS-IS Parameters** ........................ 455
  - **Configuring IS-IS Configuration Commands** .................. 477
  - **Generic Commands** .............................................. 475
  - **IS-IS Commands** ................................................ 477
  - **Show Commands** ................................................ 505
  - **Clear Commands** ................................................ 536
  - **Debug Commands** ................................................ 538
  - **Modifying Router-Level Parameters** .......................... 452
  - **Enabling IS-IS** ................................................ 452
  - **Disabling IS-IS** ............................................... 461
  - **Removing IS-IS** ............................................... 461
  - **Modifying Global IS-IS Parameters** .......................... 462
  - **Modifying IS-IS Interface Parameters** ....................... 463
  - **Configuring Leaking** .......................................... 465
  - **Redistributing External IS-IS Routers** ....................... 468
  - **Specifying MAC Addresses for All IS-IS Routers** .......... 469

- **Common Configuration Tasks** .................................... 451
  - **Configuring Interface Parameters** ............................ 456
  - **Configuring Global IS-IS Parameters** ........................ 455
  - **Configuring ISO Area Addresses** ................................ 454
  - **Configuring Interface Parameters** ................................ 456
  - **Configuring IS-IS with CLI** .................................... 445
  - **Configuring IS-IS Configuration Commands** .................. 477
  - **Generic Commands** .............................................. 475
  - **IS-IS Commands** ................................................ 477
  - **Show Commands** ................................................ 505
  - **Clear Commands** ................................................ 536
  - **Debug Commands** ................................................ 538

- **Basic IS-IS Configuration** ....................................... 449
  - **Configuring IS-IS Components** ................................ 452
  - **Enabling IS-IS** ................................................ 452
  - **Disabling IS-IS** ............................................... 461
  - **Removing IS-IS** ............................................... 461
  - **Modifying Global IS-IS Parameters** .......................... 462
  - **Modifying IS-IS Interface Parameters** ....................... 463
  - **Configuring Leaking** .......................................... 465
  - **Redistributing External IS-IS Routers** ....................... 468
  - **Specifying MAC Addresses for All IS-IS Routers** .......... 469

- **IS-IS Command Reference** ....................................... 471
  - **Basic IS-IS Configuration** ..................................... 449
  - **Configuring IS-IS Components** ................................ 452
  - **Enabling IS-IS** ................................................ 452
  - **Disabling IS-IS** ............................................... 461
  - **Removing IS-IS** ............................................... 461
  - **Modifying Global IS-IS Parameters** .......................... 462
  - **Modifying IS-IS Interface Parameters** ....................... 463
  - **Configuring Leaking** .......................................... 465
  - **Redistributing External IS-IS Routers** ....................... 468
  - **Specifying MAC Addresses for All IS-IS Routers** .......... 469

- **Common Configuration Tasks** .................................... 451
  - **Configuring Interface Parameters** ............................ 456
  - **Configuring Global IS-IS Parameters** ........................ 455
  - **Configuring ISO Area Addresses** ................................ 454
  - **Configuring Interface Parameters** ................................ 456
  - **Configuring IS-IS with CLI** .................................... 445
  - **Configuring IS-IS Configuration Commands** .................. 477
  - **Generic Commands** .............................................. 475
  - **IS-IS Commands** ................................................ 477
  - **Show Commands** ................................................ 505
  - **Clear Commands** ................................................ 536
  - **Debug Commands** ................................................ 538

- **IS-IS Configuration Overview** .................................. 446
  - **Enabling IS-IS** ................................................ 452
  - **Disabling IS-IS** ............................................... 461
  - **Removing IS-IS** ............................................... 461
  - **Modifying Global IS-IS Parameters** .......................... 462
  - **Modifying IS-IS Interface Parameters** ....................... 463
  - **Configuring Leaking** .......................................... 465
  - **Redistributing External IS-IS Routers** ....................... 468
  - **Specifying MAC Addresses for All IS-IS Routers** .......... 469

- **Common Configuration Tasks** .................................... 451
  - **Configuring Interface Parameters** ............................ 456
  - **Configuring Global IS-IS Parameters** ........................ 455
  - **Configuring ISO Area Addresses** ................................ 454
  - **Configuring Interface Parameters** ................................ 456
  - **Configuring IS-IS with CLI** .................................... 445
  - **Configuring IS-IS Configuration Commands** .................. 477
  - **Generic Commands** .............................................. 475
  - **IS-IS Commands** ................................................ 477
  - **Show Commands** ................................................ 505
  - **Clear Commands** ................................................ 536
  - **Debug Commands** ................................................ 538
# Table of Contents

- BGP Decision Process .............................................. 555
  - Option to Ignore Router ID .................................... 555
  - always-compare-med Command .................................. 556
  - Option to Ignore Next-Hop Metric .............................. 557
- Best External ....................................................... 558
  - Advertisement Rules with Best External ..................... 558
- BGP Add-Path ....................................................... 559
  - Sending Multiple Paths per Prefix to Add-Paths Peers .......... 561
- BGP Fast Reroute .................................................. 562
- Command Interactions and Dependencies ......................... 567
  - Changing the Autonomous System Number ................. 567
  - Changing the Local AS Number ............................... 568
  - Changing a Confederation Number ........................... 568
  - Changing the Router ID at the Configuration Level .... 568
  - Hold Time and Keep Alive Timer Dependencies ............ 569
  - Import and Export Route Policies ............................ 570
  - Route Damping and Route Policies ............................ 570
  - AS Override ...................................................... 570
- BGP FlowSpec ...................................................... 571
  - Validating and Importing Received IPv6 Flow Routes into the Routing Table ........................................ 572
  - Propagating IPv4 Flow Routes to BGP Neighbors ............ 573
  - Using IPv4 Flow Routes to Create Dynamic IPv4 Filter Entries .................................................................. 573
- TTL Security for LDP ................................................ 575
- BGP Configuration Process Overview ............................ 576
- Configuration Notes ................................................ 577
  - General ............................................................. 577
  - BGP Defaults ....................................................... 577
  - BGP MIB Notes ...................................................... 578
  - Configuring BGP with CLI ....................................... 581
  - BGP Configuration Overview ..................................... 582
  - Preconfiguration Requirements ................................ 582
  - BGP Hierarchy ....................................................... 582
  - Internal and External BGP Configurations .................... 582
  - Basic BGP Configuration ......................................... 584
- Common Configuration Tasks ....................................... 586
  - Creating an Autonomous System ................................ 587
  - Configuring a Router ID ......................................... 588
  - BGP Confederations ............................................... 589
  - BGP Route Reflectors ............................................. 591
  - BGP Components .................................................. 593
  - Configuring Group Attributes ................................... 593
  - Configuring Neighbor Attributes ................................ 594
  - Configuring Route Reflection ................................... 595
  - Configuring a Confederation .................................... 596
- BGP Configuration Management Tasks ......................... 597
  - Modifying an AS Number ........................................ 597
  - Modifying a Confederation Number ......................... 598
  - Modifying the BGP Router ID .................................... 598
  - Modifying the Router-Level Router ID ......................... 599
### Table of Contents

- Deleting a Neighbor ............................................. 600
- Deleting Groups .................................................. 601
- BGP Command Reference ......................................... 603
  - Configuration Commands ....................................... 613
    - Generic Commands ............................................ 613
    - BGP Commands ............................................... 615
  - Other BGP-Related Commands ................................. 651
  - Show Commands ................................................ 657
  - Clear Commands ............................................... 696
  - Debug Commands .............................................. 698

### Route Policies

- Configuring Route Policies ..................................... 704
  - Policy Statements ............................................. 705
    - Default Action Behavior ................................... 706
    - Denied IP Prefixes ......................................... 706
    - Controlling Route Flapping ................................ 707
- Regular Expressions ............................................. 709
- BGP and OSPF Route Policy Support ............................ 714
  - BGP Route Policies ............................................ 715
  - Re-advertised Route Policies ................................. 716
  - Triggered Policies ............................................ 716
  - Set MED to IGP Cost using Route Policies .................. 717
  - When to Use Route Policies .................................. 718
  - Route Policy Configuration Process Overview ............... 719
  - Configuration Notes .......................................... 720
  - General ........................................................ 720
  - Configuring Route Policies with CLI ......................... 721
  - Route Policy Configuration Overview ....................... 722
    - When to Create Routing Policies ......................... 722
    - Default Route Policy Actions ............................. 723
    - Policy Evaluation .......................................... 724
    - Damping .................................................... 727
  - Basic Configurations ........................................ 728
  - Configuring Route Policy Components ....................... 730
    - Beginning the Policy Statement ............................ 731
    - Creating a Route Policy .................................... 732
    - Configuring a Default Action .............................. 733
    - Configuring an Entry ...................................... 734
    - Configuring a Community List ............................. 735
    - Configuring Damping ....................................... 736
      - Configuring a Prefix List ................................ 737
      - Configuring PIM Join/Register Policies .................. 738
      - Configuring Bootstrap Message Import and Export Policies ........................................ 740
    - Route Policy Configuration Management Tasks ............. 741
      - Editing Policy Statements and Parameters ............. 741
      - Deleting an Entry ........................................ 743
      - Deleting a Policy Statement ............................. 743
    - Route Policy Command Reference ............................ 745
Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Policy Command Reference</td>
<td>749</td>
</tr>
<tr>
<td>Generic Commands</td>
<td>749</td>
</tr>
<tr>
<td>Route Policy Options</td>
<td>751</td>
</tr>
<tr>
<td>Route Policy Damping Commands</td>
<td>754</td>
</tr>
<tr>
<td>Route Policy Prefix Commands</td>
<td>757</td>
</tr>
<tr>
<td>Route Policy Entry Match Commands</td>
<td>758</td>
</tr>
<tr>
<td>Route Policy Action Commands</td>
<td>768</td>
</tr>
<tr>
<td>Show Commands</td>
<td>777</td>
</tr>
<tr>
<td>Standards and Protocol Support</td>
<td>781</td>
</tr>
<tr>
<td>Index</td>
<td>787</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Getting Started
Table 1: Configuration Process .......................................................... 19

Multicast
Table 2: Join Filter Policy Match Conditions ....................................... 34
Table 3: Register Filter Policy Match Conditions .................................... 34
Table 4: Bundle definition and Channel Characterization .......................... 50
Table 5: CAC Constraints ................................................................. 50
Table 6: LAG/CAC Constraints ......................................................... 54

RIP
Table 7: Route Preference Defaults by Route Type .................................. 267
Table 8: RIP Neighbor Standard Output Fields ...................................... 274

OSPF
Table 9: Route Preference Defaults by Route Type .................................. 332
Table 10: Route Preference Defaults by Route Type .................................. 351
Table 11: Route Preference Defaults by Route Type .................................. 355

IS-IS
Table 12: Potential Adjacency Capabilities ........................................... 447
Table 13: Potential Adjacency Capabilities ........................................... 490

BGP
Table 14: MED Comparison with always-compare-med ............................. 556
Table 15: BGP Fast Reroute Scenarios ................................................ 562
Table 16: Subcomponents of IPv4 Flow Route NLRI ................................. 571
Table 17: IPv4 Flowspec Actions ....................................................... 572
Table 18: and IETF MIB Variations .................................................... 578
Table 19: MIB Variable with SNMP ................................................... 578

Route Policies
Table 20: Regular Expression Operators .............................................. 710
Table 21: AS Path and Community Regular Expression Examples .............. 711
Table 22: Metric Set IGP Effect .......................................................... 717
Table 23: Default Route Policy Actions ................................................ 723
LIST OF FIGURES

Multicast
Figure 1: Anycast RP for PIM-SM Implementation Example .................................................. .37
Figure 2: IP Router Configuration Flow .................................................................................... .56

RIP
Figure 3: RIP Packet Format ........................................................................................................ .235
Figure 4: RIPv1 Format ................................................................................................................ .236
Figure 5: RIPv2 Format ................................................................................................................ .236
Figure 6: RIP Configuration and Implementation Flow ................................................................. .238

OSPF
Figure 7: Backbone Area .............................................................................................................. .288
Figure 8: PEs Connected to an MPLS-VPN Super Backbone .................................................... .291
Figure 9: Sham Links .................................................................................................................... .292
Figure 10: Example Topology with Primary and LFA Routes ..................................................... .306
Figure 11: Example Topology with Broadcast Interfaces ............................................................ .307
Figure 12: OSPF Configuration and Implementation Flow .......................................................... .311
Figure 13: OSPF Areas ................................................................................................................ .377

IS-IS
Figure 14: IS-IS Routing Domain ............................................................................................... .432
Figure 15: Using Area Addresses to Form Adjacencies ............................................................... .437
Figure 16: IS-IS Configuration and Implementation Flow ............................................................ .443
Figure 17: Configuring a Level 1 Area .......................................................................................... .458
Figure 18: Configuring a Level 1/2 Area ...................................................................................... .460

BGP
Figure 19: BGP Configuration ..................................................................................................... .544
Figure 20: Fully Meshed BGP Configuration ............................................................................... .546
Figure 21: BGP Configuration with Route Reflectors ................................................................. .547
Figure 22: BGP Update Message with Path Identifier for IPv4 NLRI ........................................ .559
Figure 23: BGP Fast Reroute for Remote PE Router Failure ....................................................... .565
Figure 24: BGP Configuration and Implementation Flow ............................................................ .576
Figure 25: Confederation Network Diagram Example ................................................................. .589
Figure 26: Route Reflection Network Diagram Example .............................................................. .591

Route Policies
Figure 27: BGP Route Policy Diagram ....................................................................................... .714
Figure 28: BGP Route Policy Diagram ....................................................................................... .715
Figure 29: OSPF Route Policy Diagram ..................................................................................... .716
Figure 30: Route Policy Configuration and Implementation Flow ............................................... .719
Figure 31: Route Policy Process Example ................................................................................... .725
Figure 32: Next Policy Logic Example ......................................................................................... .726
Figure 33: Damping Example ....................................................................................................... .727
Preface

About This Guide

This guide describes routing protocols including multicast, RIP, OSPF, IS-IS, BGP, and route policies provided by the router and presents configuration and implementation examples.

This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Audience

This manual is intended for network administrators who are responsible for configuring the routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols, standards, and services described in this manual include the following:

- Multicast — IGMP and PIM-SM
- Routing Reservation Protocol (RIP)
- Open Shortest Path First (OSPF)
- Intermediate System to Intermediate System (IS-IS)
- Border Gateway Protocol (BGP)
- Route policies
List of Technical Publications

The 7450 ESS documentation set is composed of the following books:

- **7450 ESS OS Basic System Configuration Guide**
  This guide describes basic system configurations and operations.

- **7450 ESS OS System Management Guide**
  This guide describes system security and access configurations as well as event logging and accounting logs.

- **7450 ESS OS Interface Configuration Guide**
  This guide describes card, Media Dependent Adapter (MDA) and port provisioning.

- **7450 ESS OS Router Configuration Guide**
  This guide describes logical IP routing interfaces and associated attributes such as an IP address, as well as IP and MAC-based filtering, and VRRP and Cflowd.

- **7450 ESS OS Routing Protocols Guide**
  This guide provides an overview of routing concepts and provides configuration examples for RIP, OSPF, IS-IS, BGP, and route policies.

- **7450 ESS OS MPLS Guide**
  This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).

- **7450 ESS OS Services Guide**
  This guide describes how to configure service parameters such as service distribution points (SDPs), customer information, and user services.

- **7450 ESS OAM and Diagnostic Guide**
  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.

- **7450 ESS OS Triple Play Guide**
  This guide describes Triple Play services and support provided by the 7450 ESS and presents examples to configure and implement various protocols and services.

- **7450 ESS OS Quality of Service Guide**
  This guide describes how to configure Quality of Service (QoS) policy management.

- **OS Multi-Service ISA Guide**
  This guide describes services provided by integrated service adapters such as Application Assurance, ad insertion (ADI) and Network Address Translation (NAT).
Technical Support

If you purchased a service agreement for your 7450 ESS-Series router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center at:

http://www.alcatel-lucent.com/wps/portal/support
In This Chapter

This chapter provides process flow information to configure IP routing protocols.

Alcatel-Lucent 7450 ESS-Series Router Configuration Process

Table 1 lists the tasks necessary to configure RIP, OSPF, and IS-IS, BGP, and multicast protocols, and route policies. This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Configuration Process

<table>
<thead>
<tr>
<th>Area</th>
<th>Task</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol configuration</td>
<td>Configure routing protocols:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• RIP</td>
<td>RIP on page 231</td>
</tr>
<tr>
<td></td>
<td>• OSPF</td>
<td>OSPF on page 285</td>
</tr>
<tr>
<td></td>
<td>• IS-IS</td>
<td>IS-IS on page 431</td>
</tr>
<tr>
<td>Policy configuration</td>
<td>Configure route policies</td>
<td>Route Policies on page 703</td>
</tr>
<tr>
<td>Reference</td>
<td>List of IEEE, IETF, and other proprietary entities.</td>
<td>Standards and Protocol Support on page 781</td>
</tr>
</tbody>
</table>
In This Chapter

This chapter provides information about IPv6, Internet Group Management Protocol (IGMP) and Protocol Independent Multicast (PIM).

Topics in this chapter include:

- Introduction to Multicast on page 22
  → Multicast Models on page 23
- IPv6 Multicast on page 25
- Core Router Multicast Requirements on page 27
  → Internet Group Management Protocol on page 27
  → Source-Specific Multicast Groups on page 29
  → Protocol Independent Multicast Sparse Mode (PIM-SM) on page 30
  → Anycast RP for PIM-SM on page 36
  → PIM SSM on page 25
  → Multicast Listener Discovery (MLD v1 and v2) on page 25
  → Multicast Extensions to MBGP on page 39
  → Multicast Source Discovery Protocol (MSDP) on page 40
  → Multicast Connection Admission Control (MCAC) on page 48
- Multicast Configuration Process Overview on page 56
- Configuration Notes on page 57
Introduction to Multicast

IP multicast provides an effective method of many-to-many communication. Delivering unicast datagrams is fairly simple. Normally, IP packets are sent from a single source to a single recipient. The source inserts the address of the target host in the IP header destination field of an IP datagram, intermediate routers (if present) simply forward the datagram towards the target in accordance with their respective routing tables.

Sometimes distribution needs individual IP packets be delivered to multiple destinations (like audio or video streaming broadcasts). Multicast is a method of distributing datagrams sourced from one (or possibly more) host(s) to a set of receivers that may be distributed over different (sub) networks. This makes delivery of multicast datagrams significantly more complex.

Multicast sources can send a single copy of data using a single address for the entire group of recipients. The routers between the source and recipients route the data using the group address route. Multicast packets are delivered to a multicast group. A multicast group specifies a set of recipients who are interested in a particular data stream and is represented by an IP address from a specified range. Data addressed to the IP address is forwarded to the members of the group. A source host sends data to a multicast group by specifying the multicast group address in the datagram’s destination IP address. A source does not have to register in order to send data to a group nor do they need to be a member of the group.

Routers and Layer 3 switches use the Internet Group Management Protocol (IGMP) to manage membership for a multicast session. When a host wants to receive one or more multicast sessions it will send a join message for each multicast group it wants to join. When a host wants to leave a multicast group, it will send a leave message.

To extend multicast to the Internet, the multicast backbone (Mbone) is used. The Mbone is layered on top of portions of the Internet. These portions, or islands, are interconnected using tunnels. The tunnels allow multicast traffic to pass between the multicast-capable portions of the Internet. As more and more routers in the Internet are multicast-capable (and scalable) the unicast and multicast routing table will converge.

The original Mbone was based on Distance Vector Multicast Routing Protocol (DVMRP) and was very limited. The Mbone is, however, converging around the following protocol set:

- IGMP
- Protocol Independent Multicast (Sparse Mode) (PIM-SM)
- Border Gateway Protocol with multi-protocol extensions (MBGP)
- Multicast Source Discovery Protocol (MSDP)
Multicast Models

Alcatel-Lucent routers support two models to provide multicast:

- Any-Source Multicast (ASM) on page 23
- Source Specific Multicast (SSM) on page 23

Any-Source Multicast (ASM)

Any-Source Multicast (ASM) is the IP multicast service model defined in RFC 1112, Host extensions for IP Multicasting. An IP datagram is transmitted to a host group, a set of zero or more end-hosts identified by a single IP destination address (224.0.0.0 through 239.255.255.255 for IPv4). End-hosts can join and leave the group any time and there is no restriction on their location or number. This model supports multicast groups with arbitrarily many senders. Any end-host can transmit to a host group even if it is not a member of that group.

To combat the vast complexity and scaling issues that ASM represents, the IETF is developing a service model called Source Specific Multicast (SSM).

Source Specific Multicast (SSM)

The Source Specific Multicast (SSM) service model defines a channel identified by an (S,G) pair, where S is a source address and G is an SSM destination address. In contrast to the ASM model, SSM only provides network-layer support for one-to-many delivery.

The SSM service model attempts to alleviate the following deployment problems that ASM has presented:

- Address allocation — SSM defines channels on a per-source basis. For example, the channel (S1,G) is distinct from the channel (S2,G), where S1 and S2 are source addresses, and G is an SSM destination address. This averts the problem of global allocation of SSM destination addresses and makes each source independently responsible for resolving address collisions for the various channels it creates.

- Access control — SSM provides an efficient solution to the access control problem. When a receiver subscribes to an (S,G) channel, it receives data sent only by the source S. In contrast, any host can transmit to an ASM host group. At the same time, when a sender picks a channel (S,G) to transmit on, it is automatically ensured that no other sender will be transmitting on the same channel (except in the case of malicious acts such as address spoofing). This makes it harder to spam an SSM channel than an ASM multicast group.

- Handling of well-known sources — SSM requires only source-based forwarding trees. This eliminates the need for a shared tree infrastructure. In terms of the IGMP, PIM-SM,
MSDP, MBGP protocol suite, this implies that neither the RP-based shared tree infrastructure of PIM-SM nor the MSDP protocol is required. Thus, the complexity of the multicast routing infrastructure for SSM is low, making it viable for immediate deployment. Note that MBGP is still required for distribution of multicast reachability information.

- Anticipating that point-to-multipoint applications such as Internet TV will be significant in the future, the SSM model is better suited for such applications.
IPv6 Multicast

IPv6 multicast enables multicast applications over native IPv6 networks. There are two service models: Any Source Multicast (ASM) and Source Specific Multicast (SSM) which includes PIM SSM and MLD (v1 and v2). SSM does not require source discovery and only supports single source for a specific multicast stream. As a result, SSM is easier to operate in a large scale deployment that uses the one-to-many service model.

Multicast Listener Discovery (MLD v1 and v2)

MLD is the IPv6 version of IGMP. The purpose of MLD is to allow each IPv6 router to discover the presence of multicast listeners on its directly attached links, and to discover specifically which multicast groups are of interest to those neighboring nodes.

MLD is a sub-protocol of ICMPv6. MLD message types are a subset of the set of ICMPv6 messages, and MLD messages are identified in IPv6 packets by a preceding Next Header value of 58. All MLD messages are sent with a link-local IPv6 source address, a Hop Limit of 1, and an IPv6 Router Alert option in the Hop-by-Hop Options header.

Similar to IGMPv2, MLDv1 reports only include the multicast group addresses that listeners are interested in, and don’t include the source addresses. In order to work with PIM SSM model, a similar SSM translation function is required when MLDv1 is used.

SSM translation allows an IGMPv2 device to join an SSM multicast network through the router that provides such a translation capability. Currently SSM translation can done at a box level, but this does not allow a per-interface translation to be specified. SSM translation per interface offers the ability to have a same (*,G) mapped to two different (S,G) on two different interfaces to provide flexibility.

MLDv2 is backward compatible with MLDv1 and adds the ability for a node to report interest in listening to packets with a particular multicast group only from specific source addresses or from all sources except for specific source addresses.

PIM SSM

The IPv6 address family for SSM model is supported. This includes the ability to choose which RTM table to use (unicast RTM, multicast RTM, or both). OSPF3, IS-IS and static-route have extensions to support submission of routes into the IPv6 multicast RTM.
IPv6 PIM ASM

IPv6 PIM ASM is supported. All PIM ASM related functions such as bootstrap router, RP, etc., support both IPv4 and IPv6 address-families. IPv6 specific parameters are configured under `configure>router>pim>rp>ipv6`.

Embedded RP

The detailed protocol specification is defined in RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*. This RFC describes a multicast address allocation policy in which the address of the RP is encoded in the IPv6 multicast group address, and specifies a PIM-SM group-to-RP mapping to use the encoding, leveraging, and extending unicast-prefix-based addressing. This mechanism not only provides a simple solution for IPv6 inter-domain ASM but can be used as a simple solution for IPv6 intra-domain ASM with scoped multicast addresses as well. It can also be used as an automatic RP discovery mechanism in those deployment scenarios that would have previously used the Bootstrap Router protocol (BSR).
Core Router Multicast Requirements

This section describes the multicast requirements when an Alcatel-Lucent router is deployed as part of the user’s core network.

The required protocol set is as follows:

- Internet Group Management Protocol (Internet Group Management Protocol on page 27)
- Source Specific Multicast Groups (SSM on page 29)
- Protocol Independent Multicast (Sparse Mode) (PIM-SM on page 30)
- Multicast Extensions to MBGP (Multicast Extensions to MBGP on page 39)

Internet Group Management Protocol

Internet Group Management Protocol (IGMP) is used by IPv4 hosts and routers to report their IP multicast group memberships to neighboring multicast routers. A multicast router keeps a list of multicast group memberships for each attached network, and a timer for each membership.

Multicast group memberships include at least one member of a multicast group on a given attached network, not a list of all the members. With respect to each of its attached networks, a multicast router can assume one of two roles, querier or non-querier. There is normally only one querier per physical network.

A querier issues two types of queries, a general query and a group-specific query. General queries are issued to solicit membership information with regard to any multicast group. Group-specific queries are issued when a router receives a leave message from the node it perceives as the last group member remaining on that network segment.

Hosts wanting to receive a multicast session issue a multicast group membership report. These reports must be sent to all multicast enabled routers.
IGMP Versions and Interoperability Requirements

If routers run different versions of IGMP, they will negotiate the lowest common version of IGMP that is supported on their subnet and operate in that version.

Version 1 — Specified in RFC-1112, *Host extensions for IP Multicasting*, was the first widely deployed version and the first version to become an Internet standard.

Version 2 — Specified in RFC-2236, *Internet Group Management Protocol*, added support for “low leave latency”, that is, a reduction in the time it takes for a multicast router to learn that there are no longer any members of a particular group present on an attached network.

Version 3 — Specified in RFC-3376, *Internet Group Management Protocol*, adds support for source filtering, that is, the ability for a system to report interest in receiving packets only from specific source addresses, as required to support Source-Specific Multicast (See Source Specific Multicast (SSM)), or from all but specific source addresses, sent to a particular multicast address.

IGMPv3 must keep state per group per attached network. This group state consists of a filter-mode, a list of sources, and various timers. For each attached network running IGMP, a multicast router records the desired reception state for that network.

IGMP Version Transition

Alcatel-Lucent’s routers are capable of interoperating with routers and hosts running IGMPv1, IGMPv2, and/or IGMPv3. RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3)/Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction* explores some of the interoperability issues and how they affect the various routing protocols.

IGMP version 3 specifies that if at any point a router receives an older version query message on an interface that it must immediately switch into a compatibility mode with that earlier version. Since none of the previous versions of IGMP are source aware, should this occur and the interface switch to Version 1 or 2 compatibility mode, any previously learned group memberships with specific sources (learned via the IGMPv3 specific INCLUDE or EXCLUDE mechanisms) MUST be converted to non-source specific group memberships. The routing protocol will then treat this as if there is no EXCLUDE definition present.
Source-Specific Multicast Groups

IGMPv3 permits a receiver to join a group and specify that it only wants to receive traffic for a group if that traffic comes from a particular source. If a receiver does this, and no other receiver on the LAN requires all the traffic for the group, then the designated router (DR) can omit performing a (*,G) join to set up the shared tree, and instead issue a source-specific (S,G) join only.

The range of multicast addresses from 232.0.0.0 to 232.255.255.255 is currently set aside for source-specific multicast in IPv4. For groups in this range, receivers should only issue source-specific IGMPv3 joins. If a PIM router receives a non-source-specific join for a group in this range, it should ignore it.

An Alcatel-Lucent router PIM router must silently ignore a received (*,G) PIM join message where G is a multicast group address from the multicast address group range that has been explicitly configured for SSM. This occurrence should generate an event. If configured, the IGMPv2 request can be translated into IGMPv3. The router allows for the conversion of an IGMPv2 (*,G) request into a IGMPv3 (S,G) request based on manual entries. A maximum of 32 SSM ranges is supported.

IGMPv3 also permits a receiver to join a group and specify that it only wants to receive traffic for a group if that traffic does not come from a specific source or sources. In this case, the DR will perform a (*,G) join as normal, but can combine this with a prune for each of the sources the receiver does not wish to receive.
Protocol Independent Multicast Sparse Mode (PIM-SM)

PIM-SM leverages the unicast routing protocols that are used to create the unicast routing table, OSPF, IS-IS, BGP, and static routes. Because PIM uses this unicast routing information to perform the multicast forwarding function it is effectively IP protocol independent. Unlike DVMRP, PIM does not send multicast routing tables updates to its neighbors.

PIM-SM uses the unicast routing table to perform the Reverse Path Forwarding (RPF) check function instead of building up a completely independent multicast routing table.

PIM-SM only forwards data to network segments with active receivers that have explicitly requested the multicast group. PIM-SM in the ASM model initially uses a shared tree to distribute information about active sources. Depending on the configuration options, the traffic can remain on the shared tree or switch over to an optimized source distribution tree. As multicast traffic starts to flow down the shared tree, routers along the path determine if there is a better path to the source. If a more direct path exists, then the router closest to the receiver sends a join message toward the source and then reroutes the traffic along this path.

As stated above, PIM-SM relies on an underlying topology-gathering protocol to populate a routing table with routes. This routing table is called the Multicast Routing Information Base (MRIB). The routes in this table can be taken directly from the unicast routing table, or it can be different and provided by a separate routing protocol such as MBGP. Regardless of how it is created, the primary role of the MRIB in the PIM-SM protocol is to provide the next hop router along a multicast-capable path to each destination subnet. The MRIB is used to determine the next hop neighbor to whom any PIM join/prune message is sent. Data flows along the reverse path of the join messages. Thus, in contrast to the unicast RIB that specifies the next hop that a data packet would take to get to some subnet, the MRIB gives reverse-path information, and indicates the path that a multicast data packet would take from its origin subnet to the router that has the MRIB.

PIM-SM Functions

PIM-SM functions in three phases:

- Phase One on page 31
- Phase Two on page 31
- Phase Three on page 32
Phase One

In this phase, a multicast receiver expresses its interest in receiving traffic destined for a multicast group. Typically it does this using IGMP or MLD, but other mechanisms might also serve this purpose. One of the receiver’s local routers is elected as the DR for that subnet. When the expression of interest is received, the DR sends a PIM join message towards the RP for that multicast group. This join message is known as a (*,G) join because it joins group G for all sources to that group. The (*,G) join travels hop-by-hop towards the RP for the group, and in each router it passes through the multicast tree state for group G is instantiated. Eventually the (*,G) join either reaches the RP or reaches a router that already has (*,G) join state for that group. When many receivers join the group, their join messages converge on the RP and form a distribution tree for group G that is rooted at the RP. This is known as the RP tree and is also known as the shared tree because it is shared by all sources sending to that group. Join messages are resent periodically as long as the receiver remains in the group. When all receivers on a leaf-network leave the group, the DR will send a PIM (*,G) prune message towards the RP for that multicast group. However if the prune message is not sent for any reason, the state will eventually time out.

A multicast data sender starts sending data destined for a multicast group. The sender’s local router (the DR) takes those data packets, unicast-encapsulates them, and sends them directly to the RP. The RP receives these encapsulated data packets, de-encapsulates them, and forwards them onto the shared tree. The packets then follow the (*,G) multicast tree state in the routers on the RP tree, being replicated wherever the RP tree branches, and eventually reaching all the receivers for that multicast group. The process of encapsulating data packets to the RP is called registering, and the encapsulation packets are known as PIM register packets.

At the end of phase one, multicast traffic is flowing encapsulated to the RP, and then natively over the RP tree to the multicast receivers.

Phase Two

In this phase, register-encapsulation of data packets is performed. However, register-encapsulation of data packets is unsuitable for the following reasons:

- Encapsulation and de-encapsulation can be resource intensive operations for a router to perform depending on whether or not the router has appropriate hardware for the tasks.
- Traveling to the RP and then back down the shared tree can cause the packets to travel a relatively long distance to reach receivers that are close to the sender. For some applications, increased latency is unwanted.

Although register-encapsulation can continue indefinitely, for these reasons, the RP will normally switch to native forwarding. To do this, when the RP receives a register-encapsulated data packet from source S on group G, it will normally initiate an (S,G) source-specific join towards S. This join message travels hop-by-hop towards S, instantiating (S,G) multicast tree state in the routers along the path. (S,G) multicast tree state is used only to forward packets for group G if those
packets come from source S. Eventually the join message reaches S’s subnet or a router that already has (S,G) multicast tree state, and then packets from S start to flow following the (S,G) tree state towards the RP. These data packets can also reach routers with (*,G) state along the path towards the RP - if so, they can short-cut onto the RP tree at this point.

While the RP is in the process of joining the source-specific tree for S, the data packets will continue being encapsulated to the RP. When packets from S also start to arrive natively at the RP, the RP will be receiving two copies of each of these packets. At this point, the RP starts to discard the encapsulated copy of these packets and it sends a register-stop message back to S’s DR to prevent the DR unnecessarily encapsulating the packets. At the end of phase 2, traffic will be flowing natively from S along a source-specific tree to the RP and from there along the shared tree to the receivers. Where the two trees intersect, traffic can transfer from the shared RP tree to the shorter source tree.

Note that a sender can start sending before or after a receiver joins the group, and thus, phase two may occur before the shared tree to the receiver is built.

---

**Phase Three**

In this phase, the RP joins back towards the source using the shortest path tree. Although having the RP join back towards the source removes the encapsulation overhead, it does not completely optimize the forwarding paths. For many receivers the route via the RP can involve a significant detour when compared with the shortest path from the source to the receiver.

To obtain lower latencies, a router on the receiver’s LAN, typically the DR, may optionally initiate a transfer from the shared tree to a source-specific shortest-path tree (SPT). To do this, it issues an (S,G) Join towards S. This instantiates state in the routers along the path to S. Eventually this join either reaches S’s subnet or reaches a router that already has (S,G) state. When this happens, data packets from S start to flow following the (S,G) state until they reach the receiver.

At this point the receiver (or a router upstream of the receiver) will be receiving two copies of the data - one from the SPT and one from the RPT. When the first traffic starts to arrive from the SPT, the DR or upstream router starts to drop the packets for G from S that arrive via the RP tree. In addition, it sends an (S,G) prune message towards the RP. The prune message travels hop-by-hop instantiating state along the path towards the RP indicating that traffic from S for G should NOT be forwarded in this direction. The prune message is propagated until it reaches the RP or a router that still needs the traffic from S for other receivers.

By now, the receiver will be receiving traffic from S along the shortest-path tree between the receiver and S. In addition, the RP is receiving the traffic from S, but this traffic is no longer reaching the receiver along the RP tree. As far as the receiver is concerned, this is the final distribution tree.
Encapsulating Data Packets in the Register Tunnel

Conceptually, the register tunnel is an interface with a smaller MTU than the underlying IP interface towards the RP. IP fragmentation on packets forwarded on the register tunnel is performed based upon this smaller MTU. The encapsulating DR can perform path-MTU discovery to the RP to determine the effective MTU of the tunnel. This smaller MTU takes both the outer IP header and the PIM register header overhead into consideration.

PIM Bootstrap Router Mechanism

For proper operation, every PIM-SM router within a PIM domain must be able to map a particular global-scope multicast group address to the same RP. If this is not possible, then black holes can appear (this is where some receivers in the domain cannot receive some groups). A domain in this context is a contiguous set of routers that all implement PIM and are configured to operate within a common boundary.

The bootstrap router (BSR) mechanism provides a way in which viable group-to-RP mappings can be created and distributed to all the PIM-SM routers in a domain. Each candidate BSR originates bootstrap messages (BSMs). Every BSM contains a BSR priority field. Routers within the domain flood the BSMs throughout the domain. A candidate BSR that hears about a higher-priority candidate BSR suppresses its sending of further BSMs for a period of time. The single remaining candidate BSR becomes the elected BSR and its BSMs inform the other routers in the domain that it is the elected BSR.

It is adaptive, meaning that if an RP becomes unreachable, it will be detected and the mapping tables will be modified so the unreachable RP is no longer used and the new tables will be rapidly distributed throughout the domain.

PIM-SM Routing Policies

Multicast traffic can be restricted from certain source addresses by creating routing policies. Join messages can be filtered using import filters. PIM join policies can be used to reduce denial of service attacks and subsequent PIM state explosion in the router and to remove unwanted multicast streams at the edge of the network before it is carried across the core. Route policies are created in the `config-router>policy-options` context. Join and register route policy match criteria for PIM-SM can specify the following:

- Router interface or interfaces specified by name or IP address.
- Neighbor address (the source address in the IP header of the join and prune message).
- Multicast group address embedded in the join and prune message.
- Multicast source address embedded in the join and prune message.
Join policies can be used to filter PIM join messages so no *,G or S,G state will be created on the router.

**Table 2: Join Filter Policy Match Conditions**

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Matches the:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>RTR interface by name</td>
</tr>
<tr>
<td>Neighbor</td>
<td>The neighbors source address in the IP header</td>
</tr>
<tr>
<td>Group Address</td>
<td>Multicast Group address in the join/prune message</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address in the join/prune message</td>
</tr>
</tbody>
</table>

PIM register message are sent by the first hop designated router that has a direct connection to the source. This serves a dual purpose:

- Notifies the RP that a source has active data for the group
- Delivers the multicast stream in register encapsulation to the RP and its potential receivers.
- If no one has joined the group at the RP, the RP will ignore the registers.

In an environment where the sources to particular multicast groups are always known, it is possible to apply register filters at the RP to prevent any unwanted sources from transmitting multicast stream. You can apply these filters at the edge so that register data does not travel unnecessarily over the network towards the RP.

**Table 3: Register Filter Policy Match Conditions**

<table>
<thead>
<tr>
<th>Match Condition</th>
<th>Matches the:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>RTR interface by name</td>
</tr>
<tr>
<td>Group Address</td>
<td>Multicast Group address in the join/prune message</td>
</tr>
<tr>
<td>Source Address</td>
<td>Source address in the join/prune message</td>
</tr>
</tbody>
</table>
Reverse Path Forwarding Checks

Multicast implements a reverse path forwarding check (RPF). RPF checks the path that multicast packets take between their sources and the destinations to prevent loops. Multicast requires that an incoming interface is the outgoing interface used by unicast routing to reach the source of the multicast packet. RPF forwards a multicast packet only if it is received on an interface that is used by the router to route to the source.

If the forwarding paths are modified due to routing topology changes then any dynamic filters that may have been applied must be re-evaluated. If filters are removed then the associated alarms are also cleared.
Anycast RP for PIM-SM

The implementation of Anycast RP for PIM-SM environments enable fast convergence when a PIM rendezvous point (RP) router fails by allowing receivers and sources to rendezvous at the closest RP. It allows an arbitrary number of RPs per group in a single shared-tree protocol Independent Multicast-Sparse Mode (PIM-SM) domain. This is, in particular, important for triple play configurations that opt to distribute multicast traffic using PIM-SM, not SSM. In this case, RP convergence must be fast enough to avoid the loss of multicast streams which could cause loss of TV delivery to the end customer.

Anycast RP for PIM-SM environments is supported in the base routing/PIM-SM instance of the service router. In the 7710 SR and 7750 SR product lines, this feature is supported in Layer 3-VPRN instances that are configured with PIM.

Implementation

The Anycast RP for PIM-SM implementation is defined in draft-ietf-pim-anycast-rp-03, Anycast-RP using PIM, and is similar to that described in RFC 3446, Anycast RP Mechanism Using PIM and MSDP, and extends the register mechanism in PIM so Anycast RP functionality can be retained without using Multicast Source Discovery Protocol (MSDP) (see on page 40).

The mechanism works as follows:

• An IP address is chosen to use as the RP address. This address is statically configured, or distributed using a dynamic protocol, to all PIM routers throughout the domain.

• A set of routers in the domain are chosen to act as RPs for this RP address. These routers are called the Anycast-RP set.

• Each router in the Anycast-RP set is configured with a loopback interface using the RP address.

• Each router in the Anycast-RP set also needs a separate IP address to be used for communication between the RPs.

• The RP address, or a prefix that covers the RP address, is injected into the unicast routing system inside of the domain.

• Each router in the Anycast-RP set is configured with the addresses of all other routers in the Anycast-RP set. This must be consistently configured in all RPs in the set.
Figure 1: Anycast RP for PIM-SM Implementation Example

Assume the scenario in Figure 1 is completely connected where R1A, R1B, and R2 are receivers for a group, and S1 and S2 send to that group. Assume RP1, RP2, and RP3 are all assigned the same IP address which is used as the Anycast-RP address (for example, the IP address is RPA).

Note, the address used for the RP address in the domain (the Anycast-RP address) must be different than the addresses used by the Anycast-RP routers to communicate with each other.

The following procedure is used when S1 starts sourcing traffic:

- S1 sends a multicast packet.
- The DR directly attached to S1 will form a PIM register message to send to the Anycast-RP address (RPA). The unicast routing system will deliver the PIM register message to the nearest RP, in this case RP1A.
- RP1 will receive the PIM register message, de-encapsulate it, send the packet down the shared-tree to get the packet to receivers R1A and R1B.
- RP1 is configured with RP2 and RP3’s IP address. Since the register message did not come from one of the RPs in the anycast-RP set, RP1 assumes the packet came from a DR. If the register message is not addressed to the Anycast-RP address, an error has occurred and it should be rate-limited logged.
- RP1 will then send a copy of the register message from S1’s DR to both RP2 and RP3. RP1 will use its own IP address as the source address for the PIM register message.
- RP1 may join back to the source-tree by triggering a (S1,G) Join message toward S1. However, RP1 must create (S1,G) state.
- RP2 receives the register message from RP1, de-encapsulates it, and also sends the packet down the shared-tree to get the packet to receiver R2.
- RP2 sends a register-stop message back to the RP1. RP2 may wait to send the register-stop message if it decides to join the source-tree. RP2 should wait until it has received data from the source on the source-tree before sending the register-stop message.
decides to wait, the register-stop message will be sent when the next register is received. If RP2 decides not to wait, the register-stop message is sent now.

- RP2 may join back to the source-tree by triggering a (S1,G) Join message toward S1. However, RP2 must create (S1,G) state.
- RP3 receives the register message from RP1, de-encapsulates it, but since there are no receivers joined for the group, it can discard the packet.
- RP3 sends a register-stop message back to the RP1.
- RP3 creates (S1,G) state so when a receiver joins after S1 starts sending, RP3 can join quickly to the source-tree for S1.
- RP1 processes the register-stop message from each of RP2 and RP3. RP1 may cache on a per-RP/per-(S,G) basis the receipt of register-stop message messages from the RPs in the anycast-RP set. This option is performed to increase the reliability of register message delivery to each RP. When this option is used, subsequent register messages received by RP1 are sent only to the RPs in the Anycast-RP set which have not previously sent register-stop message messages for the (S,G) entry.
- RP1 sends a register-stop message back to the DR the next time a register message is received from the DR and (when the option in the last bullet is in use) if all RPs in the Anycast-RP set have returned register-stop messages for a particular (S,G) route.

The procedure for S2 sending follows the same as above but it is RP3 which sends a copy of the register originated by S2’s DR to RP1 and RP2. Therefore, this example shows how sources anywhere in the domain, associated with different RPs, can reach all receivers, also associated with different RPs, in the same domain.
Multicast Extensions to MBGP

This section describes the implementation of extensions to MBGP to support multicast. Rather than assuming that all unicast routes are multicast-capable, some routed environments, in some cases, some ISPs do not support or have limited support for multicast throughout their AS.

BGP is capable of supporting two sets of routing information, one set for unicast routing and the other for multicast routing. The unicast and multicast routing sets either partially or fully overlay one another. To achieve this, BGP has added support for IPv4 and mcast-IPv4 address families. Routing policies can be imported or exported.

The multicast routing information can subsequently be used by the Protocol Independent Multicast (PIM) protocol to perform its Reverse Path Forwarding (RPF) lookups for multicast-capable sources. Thus, multicast traffic can only be routed across a multicast topology and not a unicast topology.

MBGP Multicast Topology Support

Recursive Lookup for BGP Next Hops

The next hop for multicast RPF routes learned by MBGP is not always the address of a directly-connected neighbor. For unicast routing, a router resolves the directly-connected next-hop by repeating the IGP routes. For multicast RPF routes, there are different ways to find the real next-hops.

- Scanning to see if a route encompasses the BGP next hop. If one exists, this route is used. If not, the tables are scanned for the best matching route.
- Check to see if the recursed next hop is taken from the protocol routing table with the lowest administrative distance (protocol preference). This means that the operating system algorithm must preform multiple lookups in the order of the lowest admin distance. Note that unlike recursion on the unicast routing table, the longest prefix match rule does not take effect; protocol preference is considered prior to prefix length. For example, the route 12.0.0.0/14 learned via MBGP will be selected over the route 12.0.0.0/16 learned via BGP.
Multicast Source Discovery Protocol (MSDP)

MSDP-speaking routers in a PIM-SM (RFC 2362, Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification) domain have MSDP peering relationship with MSDP peers in another domain. The peering relationship is made up of a TCP connection in which control information is exchanged. Each domain has one or more connections to this virtual topology.

When a PIM-SM RP learns about a new multicast source within its own domain from a standard PIM register mechanism, it encapsulates the first data packet in an MSDP source-active message and sends it to all MSDP peers.

The source-active message is flooded (after an RPF check) by each peer to its MSDP peers until the source-active message reaches every MSDP router in the interconnected networks. If the receiving MSDP peer is an RP, and the RP has a (*.G) entry (receiver) for the group, the RP creates state for the source and joins to the shortest path tree for the source. The encapsulated data is de-encapsulated and forwarded down the shared tree of that RP. When the packet is received by the last hop router of the receiver, the last hop router also may join the shortest path tree to the source.

The MSDP speaker periodically sends source-active messages that include all sources.

Anycast RP for MSDP

MSDP is a mechanism that allows rendezvous points to share information about active sources. When RPs in remote domains hear about the active sources, they can pass on that information to the local receivers and multicast data can be forwarded between the domains. MSDP allows each domain to maintain an independent RP that does not rely on other domains but enables RPs to forward traffic between domains. PIM-SM is used to forward the traffic between the multicast domains.

Using PIM-SM, multicast sources and receivers register with their local RP by the closest multicast router. The RP maintains information about the sources and receivers for any particular group. RPs in other domains do not have any knowledge about sources located in other domains.

MSDP is required to provide inter-domain multicast services using Any Source Multicast (ASM). Anycast RP for MSDP enables fast convergence when should an MSDP/PIM PR router fail by allowing receivers and sources to rendezvous at the closest RP.
**MSDP Procedure**

When an RP in a PIM-SM domain first learns of a new sender, for example, by PIM register messages, it constructs a source-active (SA) message and sends it to its MSDP peers. The SA message contains the following fields:

- Source address of the data source
- Group address the data source sends to
- IP address of the RP

Note that an RP that is not a designated router on a shared network do not originate SAs for directly-connected sources on that shared network. It only originates in response to receiving register messages from the designated router.

Each MSDP peer receives and forwards the message away from the RP address in a peer-RPF flooding fashion. The notion of peer-RPF flooding is with respect to forwarding SA messages. The Multicast RPF Routing Information Base (MRIB) is examined to determine which peer towards the originating RP of the SA message is selected. Such a peer is called an RPF peer.

If the MSDP peer receives the SA from a non-RPF peer towards the originating RP, it will drop the message. Otherwise, it forwards the message to all its MSDP peers (except the one from which it received the SA message).

When an MSDP peer which is also an RP for its own domain receives a new SA message, it determines if there are any group members within the domain interested in any group described by an (S,G) entry within the SA message. That is, the RP checks for a (*,G) entry with a non-empty outgoing interface list. This implies that some system in the domain is interested in the group. In this case, the RP triggers an (S,G) join event toward the data source as if a join/prune message was received addressed to the RP. This sets up a branch of the source-tree to this domain. Subsequent data packets arrive at the RP by this tree branch and are forwarded down the shared-tree inside the domain. If leaf routers choose to join the source-tree they have the option to do so according to existing PIM-SM conventions. If an RP in a domain receives a PIM join message for a new group G, the RP must trigger an (S,G) join event for each active (S,G) for that group in its SA cache.

This procedure is called flood-and-join because if any RP is not interested in the group, the SA message can be ignored, otherwise, they join a distribution tree.
MSDP Peering Scenarios

Draft-ietf-mboned-msdp-deploy-nn.txt, Multicast Source Discovery Protocol (MSDP) Deployment Scenarios, describes how protocols work together to provide intra- and inter-domain ASM service.

Inter-domain peering:

- Peering between PIM border routers (single-hop peering)
- Peering between non-border routers (multi-hop peering)
- MSDP peering without BGP
- MSDP peering between mesh groups
- MSDP peering at a multicast exchange

Intra-domain peering:

- Peering between routers configured for both MSDP and MBGP
- MSDP peer is not BGP peer (meaning, no BGP peer)

MSDP Peer Groups

MSDP peer groups are typically created when multiple peers have a set of common operational parameters. Group parameters not specifically configured are inherited from the global level.

MSDP Mesh Groups

MSDP mesh groups are used to reduce source active flooding primarily in intra-domain configurations. When a number of speakers in an MSDP domain are fully meshed they can be configured as a mesh group. The originator of the source active message forwards the message to all members of the mesh group. Because of this, forwarding the SA between non-originating members of the mesh group is not necessary.
MSDP Routing Policies

MSDP routing policies allow for filtering of inbound and/or outbound active source messages. Policies can be configured at different levels:

- Global level — Applies to all peers
- Group level — Applies to all peers in peer-group
- Neighbor level — Applies only to specified peer

The most specific level is used. If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If no policy is applied source active messages are passed.

Match conditions include:

- Neighbor — Matches on a neighbor address is the source address in the IP header of the source active message.
- Route filter — Matches on a multicast group address embedded in the source active message
- Source address filter — Matches on a multicast source address embedded in the source active message
Multicast in Virtual Private Networks

Draft Rosen

RFC2547bis, BGP/MPLS IP VPNs, describes a method of providing a VPN service. A VPN provides secure connections to the network, allowing more efficient service to remote users without compromising the security of firewalls. The Rosen draft specifies the protocols and procedures which must be implemented in order for a service provider to provide a unicast VPN. The draft extends that specification by describing the protocols and procedures which a service provider must implement in order to support multicast traffic in a VPN, assuming that PIM [PIMv2] is the multicast routing protocol used within the VPN, and the SP network can provide PIM as well.

IGMP is not supported for receivers or senders directly attached to the PE.

For further information, refer to the Virtual Private Routed Network Service section of the Services Guide.
Multicast Debugging Tools

This section describes multicast debugging tools requirement for the router family of products. The debugging tools for multicast consist out of three elements; mtrace, mstat, and mrinfo.

Mtrace

Assessing problems in the distribution of IP multicast traffic can be difficult. The mtrace feature utilizes a tracing feature implemented in multicast routers that is accessed via an extension to the IGMP protocol. The mtrace feature is used to print the path from the source to a receiver; it does this by passing a trace query hop-by-hop along the reverse path from the receiver to the source. At each hop, information such as the hop address, routing error conditions and packet statistics should be gathered and returned to the requestor.

Data added by each hop includes:

- Query arrival time
- Incoming interface
- Outgoing interface
- Previous hop router address
- Input packet count
- Output packet count
- Total packets for this source/group
- Routing protocol
- TTL threshold
- Forwarding/error code

The information enables the network administrator to determine:

- Where multicast flows stop
- the flow of the multicast stream

When the trace response packet reaches the first hop router (the router that is directly connected to the source’s net), that router sends the completed response to the response destination (receiver) address specified in the trace query.

If some multicast router along the path does not implement the multicast traceroute feature or if there is some outage, then no response is returned. To solve this problem, the trace query includes
a maximum hop count field to limit the number of hops traced before the response is returned. This allows a partial path to be traced.

The reports inserted by each router contain not only the address of the hop, but also the TTL required to forward and some flags to indicate routing errors, plus counts of the total number of packets on the incoming and outgoing interfaces and those forwarded for the specified group. Taking differences in these counts for two traces separated in time and comparing the output packet counts from one hop with the input packet counts of the next hop allows the calculation of packet rate and packet loss statistics for each hop to isolate congestion problems.

Finding the Last Hop Router

The trace query must be sent to the multicast router which is the last hop on the path from the source to the receiver. If the receiver is on the local subnet (as determined using the subnet mask), then the default method is to multicast the trace query to all-routers.mcast.net (224.0.0.2) with a TTL of 1. Otherwise, the trace query is multicast to the group address since the last hop router will be a member of that group if the receiver is. Therefore, it is necessary to specify a group that the intended receiver has joined. This multicast is sent with a default TTL of 64, which may not be sufficient for all cases.

When tracing from a multihomed host or router, the default receiver address may not be the desired interface for the path from the source. In that case, the desired interface should be specified explicitly as the receiver.

Directing the Response

By default, mtrace first attempts to trace the full reverse path, unless the number of hops to trace is explicitly set with the hop option. If there is no response within a 3 second timeout interval, a "*" is printed and the probing switches to hop-by-hop mode. Trace queries are issued starting with a maximum hop count of one and increasing by one until the full path is traced or no response is received. At each hop, multiple probes are sent. The first attempt is made with the unicast address of the host running mtrace as the destination for the response. Since the unicast route may be blocked, the remainder of attempts request that the response be multicast to mtrace.mcast.net (224.0.1.32) with the TTL set to 32 more than what’s needed to pass the thresholds seen so far along the path to the receiver. For the last attempts the TTL is increased by another 32.

Alternatively, the TTL may be set explicitly with the TTL option.

For each attempt, if no response is received within the timeout, a "*" is printed. After the specified number of attempts have failed, mtrace will try to query the next hop router with a DVMRP_ASK_NEIGHBORS2 request (as used by the mrinfo program) to determined the router type.
The output of mtrace is a short listing of the hops in the order they are queried, that is, in the reverse of the order from the source to the receiver. For each hop, a line is printed showing the hop number (counted negatively to indicate that this is the reverse path); the multicast routing protocol; the threshold required to forward data (to the previous hop in the listing as indicated by the up-arrow character); and the cumulative delay for the query to reach that hop (valid only if the clocks are synchronized). The response ends with a line showing the round-trip time which measures the interval from when the query is issued until the response is received, both derived from the local system clock.

Mtrace/mstat packets use special IGMP packets with IGMP type codes of 0x1E and 0x1F.

---

**Mstat**

The `mstat` command adds the capability to show the multicast path in a limited graphic display and provide drops, duplicates, TTLs and delays at each node. This information is useful to the network operator because it identifies nodes with high drop & duplicate counts. Duplicate counts are shown as negative drops.

The output of `mstat` provides a limited pictorial view of the path in the forward direction with data flow indicated by arrows pointing downward and the query path indicated by arrows pointing upward. For each hop, both the entry and exit addresses of the router are shown if different, along with the initial ttl required on the packet in order to be forwarded at this hop and the propagation delay across the hop assuming that the routers at both ends have synchronized clocks. The output consists of two columns, one for the overall multicast packet rate that does not contain lost/sent packets and a column for the (S,G)-specific case. The S,G statistics do not contain lost/sent packets.

---

**Mrinfo**

`mrinfo` is a simple mechanism based on the `ask_neighbors igmp` to display the configuration information from the target multicast router. The type of information displayed includes the Multicast capabilities of the router, code version, metrics, ttl-thresholds, protocols and status. This information, for instance, can be used by network operators to verify if bi-directional adjacencies exist. Once the specified multicast router responds, the configuration is displayed.
Multicast Connection Admission Control (MCAC)

Inspired by network deployments targeted at Ethernet-based triple play aggregation for residential customers, the router has implemented support for Broadcast TV (BTV) distribution. Distribution of BTV services can be facilitated in different ways, such as:

- PIM-SSM based distribution of the channels on a router aggregation network, with dynamic IGMP joins from the connected DSLAMs.
- IP-VPN based video distribution.

The capacity taken by the BTV channels may exceed the capacity of the routers to access node link (the second mile) or even the capacity of specific network links in the aggregation network (the third mile and fourth mile links). In this case, MCAC has been implemented to limit the amount of bandwidth consumed by BTV services on these links. As the bandwidth constraint can be on the second-mile link and/or on any network link, the multicast CAC function is applicable to any given interface for both IGMP and PIM, and in case of BTV distribution based on VPLS, on VPLS SAPs and SDPs, where IGMP snooping is enabled.

BTV

Broadcast TV (BTV) is the delivery of TV channels by means of multicast or broadcast to many subscribers at the same time (for example, your standard network television channels). BTV is different from Video On Demand (VOD) as this method is delivered by unicast to specific subscribers.

The capacity taken by the BTV channels may exceed the capacity of the routers to access node link (the second mile) or even the capacity of specific network links in the aggregation network (the third mile and fourth mile links).

Potentially, running the multicast CAC function might cause specific channels to be temporarily unavailable to subscribers when overloaded. However, the degradation of the quality of the BTV service offering is avoided.

Overbooking BTV video channels in Telco networks follows the MSO trend regarding “switched broadcasts” where digital broadcast programming is only offered to those nodes where and when subscribers actively request that programming. In other words, BTV channels are offered in an on-demand manner rather than being available at all times on the cable network (which is currently typical). This method enables the creation of a virtual programming capacity without the correlated physical expense of creating and dedicating spectral resources. This trend in the MSO space, that now gets ported in the Telco space, is motivated by planned expansions of the BTV programming lineups, particularly those in bandwidth-hungry high definition television format.
The SR OS allows for some form of CAC for BTV, as it allows limiting the maximum number of channels that can be distributed on a given IP interface (for IGMP and PIM) or VPLS SAP/SDP (with IGMP- snooping). However, this level of control, basically first-come-first-service, is not sufficient in an environment where not all channels are equal in their priority and bandwidth usage.

- Simply performing CAC based on a number of channels does not effectively limit the amount of bandwidth consumed by BTV on any given link as there may be a mix of Standard Definition (SD) and High Definition (HD) channels being offered, or mix of MPEG2/MPEG4 SD channels.

To accommodate BTV CAC requirements, the router implements multicast CAC policies that can be applied to an IP interface or VPLS SAP/SDPs. This allows:

- Definition of BTV bundles:
  - Grouping of MC-group addresses into bundles. Each MC channel can only belong to one specific bundle within the context of one specific policy.
  - Characterization of channels:
    - Bandwidth — Allows differentiation between, for example, SD and HD channels, MPEG2 and MPEG4.
    - Channel type — Either mandatory (can never be blocked, and therefore the CAC algorithm assumes that the bandwidth is permanently reserved) or optional (subject to CAC. This may be temporarily unavailable in times of congestion.).
    - Channel class — For LAG, the class parameter allows further prioritizing of the mandatory or optional channels. This brings the number of priority levels to four during reshuffles of the joined channels when LAG ports are changing state.

- CAC constraints:
  - Interface — Defines constraints on the total amount of bandwidth allowed for BTV on a given IP interface for VPLS SAP/SDP entities.
  - Bundle constraints — Defines constraints on amount of bandwidth per bundle that is allowed on a given IP interface or VPLS SAP/SDP entities.
  - Note that the constraint of the total amount of multicast traffic per channel class is implicit.
  - CAC constraints take into account the potential use of LAG on access or network ports.

Based on these constraints, router multicast CAC can accept or refuse individual IGMP/PIM joins received on such interface (ingress CAC).

It is important to realize that all CAC functionality is based on configuration rather than measured/real bandwidth.
Table 4 displays an example configuration. Table 5 displays CAC constraints.

Table 4: Bundle definition and Channel Characterization

<table>
<thead>
<tr>
<th>BTV Channel</th>
<th>Bandwidth in Mbps</th>
<th>Channel Type</th>
<th>Channel Class</th>
<th>Bundle</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.1.1.1</td>
<td>4,0</td>
<td>Mandatory</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>224.1.1.6</td>
<td>14,0</td>
<td>Optional</td>
<td>Low</td>
<td>2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Table 5: CAC Constraints

<table>
<thead>
<tr>
<th>Allowed Bandwidth in Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
</tr>
<tr>
<td>Bundle 1</td>
</tr>
<tr>
<td>Bundle 2</td>
</tr>
<tr>
<td>...</td>
</tr>
</tbody>
</table>
CAC Algorithm

The multicast CAC algorithm only applies to:

- Channels that have not yet been distributed and that are characterized as optional. Bandwidth for channels characterized as mandatory is pre-reserved on the bundle level and configured on interface level. Channels that are already being distributed will not be dropped.
- Channels specified in the CAC policy. Multicast channels not specified in the CAC policy are not subject to multicast CAC. Treatment of such unspecified channels is configurable as either accept or discard.

The CAC algorithm is applied at both the interface level and the bundle level CAC constraints specified in the policy. Both checks must pass before the channel is allowed.

When evaluating the channels to forward when starting the policy, the available bandwidth fairness between different bundles is maintained and the following applies:

- Mandatory high bundle-1, Mandatory high bundle-2, Mandatory high bundle-3, Mandatory high bundle, and so on.
- Mandatory low bundle-1, Mandatory low bundle-2, Mandatory low bundle-3, Mandatory low bundle, and so on.
- Optional high bundle-1, Optional high bundle-2, Optional high bundle-3, Optional high bundle, and so on.
- Optional low bundle-1, Optional low bundle-2, Optional low bundle-3, Optional low bundle, and so on.

This method does not guarantee that all bundles are fully allocated while others are not. However it does ensure that all mandatory high channels are allocated before any mandatory lows are allocated.
Interface-Level CAC

Interface-level CAC constraints are applied to the interface on which the request was received.

The channel is allowed if:

- The channel is characterized as mandatory and the bandwidth for the already distributed mandatory channels plus the bandwidth of this mandatory channel is not greater than the configured amount of mandatory bandwidth.
- The channel is characterized as optional and the bandwidth for the already distributed optional channels plus the bandwidth of this optional channel is not greater than the configured amount of unconstrained-bw, the configured amount of mandatory bandwidth.

No bandwidth (channels) can be allocated once the configured maximum bandwidth for a given interface has been exceeded.

Bundle-Level CAC

Bundle-level CAC is applied to the bundle to which the channel belongs that triggered the CAC algorithm.

The channel is allowed if:

- When it is characterized as mandatory
- When it is an optional channel then the configured bundle bandwidth cannot get exceeded by the distributed bandwidth. The distributed bandwidth equals the bandwidth of all the mandatory channels belonging to that bundle plus the bandwidth of the optional channels being distributed plus the bandwidth of the optional channel that want to join.
Dealing with Configuration Changes

The system handles changes in the BTV bundle definition and CAC constraints efficiently, without dropping any active channels (even when the constraints have become more stringent).

More stringent constraint examples are:

- An operator adds additional mandatory channels to the BTV bundle definition (in which bandwidth needs to be pre-reserved).
- An operator changes a currently inactive channel from an optional to a mandatory state.
- An operator reduces the allowed bandwidth for one of the bundles or at the interface level.
- An operator moves channels between bundles.

When these changes become active, all currently active channels continue to be forwarded until they are explicitly released. Channels are not dropped as a result of such policy changes. Additional joins for optional channels are refused until sufficient bandwidth is available to support the more stringent constraints, at which point they become active. Additional joins for existing mandatory channels are never refused.

If a new mandatory channel is defined, or if a currently inactive channel is reconfigured from optional to mandatory, then it will not become active and joins for it will be refused until sufficient bandwidth is available on the link and bundle to enable it.

If the allowed bandwidth is reduced at the interface or bundle level, all active channels are maintained. New joins for optional channels are refused until the new levels are reached.
LAG Interworking

LAG may be used on the second mile (from a DSLAM to an SR-OS node) or on trunk networks.

The CAC policy, which is applied on an interface or VPLS SAP/SDP level, may have to be re-evaluated when one of the component links fails (i.e. in the case that BTV multipoint traffic would in normal mode be hashed across the component links).

- The CAC policy allows specifying the amount of component links used for BTV distribution in normal operation as well as the available BTV bandwidth in normal mode of operation on an interface and bundle level.
- The CAC constraints to be applied in degraded mode can be explicitly configured for the interface/bundle. There are multiple constraint-levels defined that can be selected depending on the severity of the failure.

The set of CAC constraints to be used is automatically determined based on the remaining number of operational links. The operation links determine the weight level for the LAG group. The CAC constraints definition specify the weight level to which they apply.

For a LAG of three or more component links (where three CAC constraint levels could be applied), the CAC constraints in the policy could look like:

<table>
<thead>
<tr>
<th>Weight (tbc)</th>
<th>Allowed Bandwidth in Mbps (normal mode)</th>
<th>Allowed Bandwidth in Mbps (degraded mode 1)</th>
<th>Allowed Bandwidth in Mbps (degraded mode 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>&gt;=10</td>
<td>&gt;=6</td>
<td>&gt;=2</td>
</tr>
<tr>
<td>Bundle 1</td>
<td>750</td>
<td>400</td>
<td>200</td>
</tr>
<tr>
<td>Bundle 2</td>
<td>580</td>
<td>300</td>
<td>200</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Table 6: LAG/CAC Constraints

In the case of reduction of available bandwidth (for example, a component link failure), CAC attempts to fit all mandatory channels. This is performed by re-evaluating the mandatory channels in an arbitrary order using the same two-level CAC algorithm applied at the interface and bundle levels, and using the constraints for the degraded mode of operation. If there is not sufficient capacity to carry all mandatory channels in this degraded mode, some are channels will be dropped. If capacity for BTV is remaining, then subsequently all optional channels are re-evaluated in an arbitrary order. Distribution of some of them may be stopped as a consequence.
When a previously failed link becomes re-operational then the CAC algorithm takes into account the return to the normally configured bandwidth, and as a result, starts accepting more optional channels again.

CAC Policy for Split Horizon Groups

When IGMP snooping on residential SAPs was introduced enabling multicast CAC policies to be applied to split horizon groups. When a CAC policies are applied to a split horizon group then member SAPs do not permit policy enforcement configurations.
Figure 2 displays the process to configure multicast parameters.

![IP Router Configuration Flow Diagram]

**Figure 2: IP Router Configuration Flow**
Configuration Notes

This section describes multicast configuration caveats.

General

- A multicast stream is required by one of more multicast clients.
- A multicast stream is offered by one or more multicast servers.
Configuring Multicast Parameters with CLI

This section provides information to configure multicast, IGMP, and PIM.

Topics in this section include:

- Multicast Configuration Overview on page 60
- Basic Configuration on page 61
- Common Configuration Tasks on page 64
- Service Management Tasks on page 81
Multicast Configuration Overview

The routers use IGMP to manage membership for a given multicast session. IGMP is not enabled by default. When enabled, at least one interface must be specified in the IGMP context as IGMP is an interface function. Creating an interface enables IGMP. Traffic can only flow away from the router to an IGMP interface and to and from a PIM interface. A router directly connected to a source must have PIM enabled on the interface to that source. The traffic travels in a network from PIM interface to PIM interface and arrives finally on an IGMP enabled interface.

The IGMP CLI context allows you to specify an existing IP interface and modify the interface-specific parameters. Static IGMP group memberships can be configured to test multicast forwarding without a receiver host. When IGMP static group membership is enabled, data is forwarded to an interface without receiving membership reports from host members.

When static IGMP group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static IGMP group entries do not generate join messages toward the RP. When a host wants to receive multicast sessions it sends a join message for each multicast group it wants to join. Then, a leave message may be sent for each multicast group it no longer wishes to participate with.

A multicast router keeps a list of multicast group memberships for each attached network, and an interval timer for each membership. Hosts issue a Multicast Group Membership Report when they want to receive a multicast session. The reports are sent to all multicast routers.

PIM is not enabled by default. When PIM is enabled, data is forwarded to network segments with active receivers that have explicitly requested the multicast group. When enabled, at least one interface must be specified in the PIM context as PIM is an interface function. Creating an interface enables PIM.
Basic Configuration

Perform the following basic multicast configuration tasks:

For IGMP:

- Enable IGMP (required)
- Configure IGMP interfaces (required)
- Specify IGMP version on the interface (optional)
- Configure static (S,G)/(*,G) (optional)
- Configure SSM translation (optional)

For PIM:

- Enable PIM (required)
- Add interfaces so the protocol establishes adjacencies with the neighboring routers (required)
- Configure a way to calculate group-to-RP mapping (required) by either:
  - Static group-to-RP mapping
  - Enable Candidate RP/Bootstrap mechanism on some routers.
- Enable unicast routing protocols to learn routes towards the RP/source for reverse path forwarding (required)
- Add SSM ranges (optional)
- Enable Candidate BSR (optional)
- Enable Candidate RP (optional)
- Change hello interval (optional)
- Configure route policies (bootstrap-export, bootstrap-import, import join and register)

For MSDP:

- Enable MSDP (required)
- Configure peer
- Configure local address

For MCAC:

- Configure policy name
- Configure bundle parameters
- Specify default action
The following example displays the enabled IGMP and PIM configurations:

A:LAX>config>router>igmp# info
----------------------------------------------
interface "lax-vls"
exit
interface "p1-ix"
exit
----------------------------------------------
A:LAX>config>router>igmp# info detail
----------------------------------------------
interface "lax-vls"
  no import
  version 3
  no shutdown
exit
interface "p1-ix"
  no import
  version 3
  no shutdown
exit
query-interval 125
query-last-member-interval 1
query-response-interval 10
robust-count 2
no shutdown
----------------------------------------------
A:LAX>config>router>igmp# exit
A:LAX>config>router# pim
A:LAX>config>router>pim# info
----------------------------------------------
interface "system"
exit
interface "lax-vls"
exit
interface "lax-sjc"
exit
interface "p1-ix"
exit
rp
  static
    address 2.22.187.237
    group-prefix 224.24.24.24/32
exit
exit
bsr-candidate
  shutdown
exit
rp-candidate
  shutdown
exit
exit
----------------------------------------------
A:LAX>config>router>pim# info detail
----------------------------------------------
no import join-policy
no import register-policy
interface "system"
interface "lax-vls"
  priority 1
  hello-interval 30
  multicast-senders auto
  no tracking-support
  bsm-check-rtr-alert
  no shutdown
exit

interface "lax-sjc"
  priority 1
  hello-interval 30
  multicast-senders auto
  no tracking-support
  bsm-check-rtr-alert
  no shutdown
exit

interface "p1-ix"
  priority 1
  hello-interval 30
  multicast-senders auto
  no tracking-support
  bsm-check-rtr-alert
  no shutdown
exit

apply-to none

rp
  no bootstrap-import
  no bootstrap-export
  static
    address 2.22.187.237
    no override
    group-prefix 224.24.24.24/32
  exit

exit

bsr-candidate
  shutdown
  priority 0
  hash-mask-len 30
  no address
exit

rp-candidate
  shutdown
  no address
  holdtime 150
  priority 192
exit

exit

no shutdown

A:LAX>config>router>pim#
Common Configuration Tasks

The following sections describe basic multicast configuration tasks.

- Configuring IGMP Parameters on page 64
  → Enabling IGMP on page 64
  → Configuring an IGMP Interface on page 65
  → Configuring Static Parameters on page 66
  → Configuring SSM Translation on page 68
- Configuring PIM Parameters on page 69
  → Enabling PIM on page 69
  → Configuring PIM Interface Parameters on page 70
  → Importing PIM Join/Register Policies on page 75
- Configuring Multicast Source Discovery Protocol (MSDP) Parameters on page 77
- Configuring MCAC Parameters on page 78
- Disabling IGMP or PIM on page 81

---

Configuring IGMP Parameters

---

Enabling IGMP

Use the following CLI syntax to enable IGMP.

CLI Syntax: `config>router# igmp`

The following example displays the detailed output when IGMP is enabled.

```
A:LAX>>config>router# info detail
...  #------------------------------------------
    echo "IGMP Configuration"
    #------------------------------------------
    igmp
    query-interval 125
    query-last-member-interval 1
    query-response-interval 10
    robust-count 2
    no shutdown
    exit
    #------------------------------------------
A:LAX>>config>system#
```
Configuring an IGMP Interface

To configure an IGMP interface:

**CLI Syntax:**

```
config>router# igmp
   interface ip-int-name
   max-groups value
   import policy-name
   version version
   no shutdown
```

Use the following CLI syntax to configure IGMP interfaces:

**Example:**

```
config>router# igmp
   interface "lax-vls"
config>router>igmp>if? no shutdown
config>router>igmp>if# exit
config>router>igmp# interface "p1-ix"
config>router>igmp>if? no shutdown
config>router>igmp>if# exit
config>router>igmp# interface "lax-sjc"
config>router>igmp>if? no shutdown
config>router>igmp>if# exit
```

The following example displays the IGMP configuration:

```
A:LAX>config>router>igmp# info
---------------------------------------
   interface "lax-sjc"
   exit
   interface "lax-vls"
   exit
   interface "p1-ix"
   exit
---------------------------------------
A:LAX>config>router>igmp# exit
```
Configuring Static Parameters

To add an IGMP static multicast source:

**CLI Syntax:**
```
config>router# igmp
   interface ip-int-name
       no shutdown
       static
       group grp-ip-address
       source ip-address
```

Use the following CLI syntax to configure static group addresses and source addresses for the SSM translate group ranges:

**Example:**
```
config>router>igmp# interface lax-vls
config>router>igmp>if# static
config>router>igmp>if>static# group 229.255.0.2
config>router>igmp>if>static>group# source 172.22.184.197
config>router>igmp>if>static>group# exit
config>router>igmp>if>static# exit
config>router>igmp>if# exit
```

The following example displays the configuration:

```
A:LAX>config>router>igmp# info
----------------------------------------------
   interface "lax-sjc"
       exit
   interface "lax-vls"
       static
       group 229.255.0.2
       source 172.22.184.197
       exit
   exit
   interface "p1-ix"
       exit
----------------------------------------------
A:LAX>config>router>igmp#
```
To add an IGMP static starg entry:

**CLI Syntax:**
```
config>router# igmp
    interface ip-int-name
        no shutdown
        static
            group grp-ip-address
        starg
```

Use the following CLI syntax to configure static group addresses and add a static (*,G) entry:

**Example:**
```
config>router>igmp# interface lax-sjc
config>router>igmp>if# static
config>router>igmp>if>static# group 230.1.1.1
config>router>igmp>if>static>group# starg
config>router>igmp>if>static>group# exit
config>router>igmp>if>static# exit
config>router>igmp>if# exit
config>router>igmp#
```

The following example displays the configuration:
```
A:LAX>config>router>igmp# info
----------------------------------------------
interface "lax-sjc"
    static
        group 230.1.1.1
        starg
        exit
        exit
exit
interface "lax-vls"
    static
        group 229.255.0.2
        source 172.22.184.197
        exit
        exit
exit
interface "p1-ix"
    exit
----------------------------------------------
A:LAX>config>router>igmp#
```
Configuring SSM Translation

To configure IGMP parameters:

**CLI Syntax:**
```
config>router# igmp
    ssm-translate
        grp-range start end
        source ip-address
```

The following example displays the command usage to configure IGMP parameters:

**Example:**
```
config>router# igmp
config>router>igmp# ssm-translate
config>router>igmp>ssm# grp-range 229.255.0.1 231.2.2.2
config>router>igmp>ssm>grp-range# source 10.1.1.1
```

The following example displays the SSM translation configuration:

```
A:LAX>config>router>igmp# info
----------------------------------------------
ssm-translate
    grp-range 229.255.0.1 231.2.2.2
        source 10.1.1.1
    exit
exit
interface "lax-sjc"
    static
        group 230.1.1.1
            starg
        exit
exit
interface "lax-vls"
    static
        group 229.255.0.2
            source 172.22.184.197
        exit
exit
interface "p1-ix"
exit
----------------------------------------------
A:LAX>config>router>igmp# exit
```
Configuring PIM Parameters

- Enabling PIM on page 69
- Configuring PIM Interface Parameters on page 70
- Importing PIM Join/Register Policies on page 75

Enabling PIM

When configuring PIM, make sure to enable PIM on all interfaces for the routing instance, otherwise multicast routing errors can occur.

Use the following CLI syntax to enable PIM.

**CLI Syntax:** config>router# pim

The following example displays the detailed output when PIM is enabled.

```
A:LAX>>config>router# info detail
...  
#------------------------------------------
  echo "PIM Configuration"
#------------------------------------------
  pim
    no import join-policy
    no import register-policy
    apply-to none
    rp
      no bootstrap-import
      no bootstrap-export
      static
      exit
    bsr-candidate
      shutdown
      priority 0
      hash-mask-len 30
      no address
      exit
    rp-candidate
      shutdown
      no address
      holdtime 150
      priority 192
      exit
    exit
    exit
    no shutdown
  exit
#------------------------------------------
...  
A:LAX>>config>system#
```
Configuring PIM Interface Parameters

The following example displays the command usage to configure PIM interface parameters:

**Example**: A:LAX>config>router# pim
A:LAX>config>router>pim# interface "system"
A:LAX>config>router>pim# interface "lax-vls"
A:LAX>config>router>pim# interface "lax-sjc"
A:LAX>config>router>pim# interface "p1-ix"
A:LAX>config>router>pim# rp
A:LAX>config>router>pim>rp# static
A:LAX>config>router>pim>rp# static address 2.22.187.237
A:LAX>config>router>pim>rp# static group-prefix 224.24.24.24/32
A:LAX>config>router>pim>rp# static exit
A:LAX>config>router>pim>rp# static exit
A:LAX>config>router>pim> rp
A:LAX>config>router>pim#

The following example displays the PIM configuration:

A:LAX>config>router>pim# info

```
----------------------------------------------
interface "system"
exit
interface "lax-vls"
exit
interface "lax-sjc"
exit
interface "p1-ix"
exit
rp
static
  address 2.22.187.237
  group-prefix 224.24.24.24/32
  exit
exit
address 10.10.10.10
exit
exit
bsr-candidate
shutdown
exit
rp-candidate
shutdown
exit
exit
----------------------------------------------
A:LAX>config>router>pim#
```
Example:

```
A:SJC>config>router>pim# pim
A:SJC>config>router>pim# interface "system"
A:SJC>config>router>pim>if# exit
A:SJC>config>router>pim# interface "sjc-lax"
A:SJC>config>router>pim>if# exit
A:SJC>config>router>pim# interface "sjc-nyc"
A:SJC>config>router>pim>if# exit
A:SJC>config>router>pim# interface "sjc-sfo"
A:SJC>config>router>pim>if# exit
A:SJC>config>router>pim# rp
A:SJC>config>router>pim>rp# static
A:SJC>config>router>pim>rp>static# address 2.22.187.237
A:SJC>config>router>pim>rp>static>address# group-prefix 224.24.24.24/32
A:SJC>config>router>pim>rp# exit
A:SJC>config>router>pim# exit
A:SJC>config>router>pim# info
```

```
----------------------------------------------
interface "system"
exit
interface "sjc-lax"
exit
interface "sjc-nyc"
exit
interface "sjc-sfo"
exit
rp
static
    address 2.22.187.237
    group-prefix 224.24.24.24/32
exit
exit
bsr-candidate
shutdown
exit
rp-candidate
shutdown
exit
exit
----------------------------------------------
A:SJC>config>router>pim#
```
Example:

A: MV>config>router# pim
A: MV>config>router>pim# interface "system"
A: MV>config>router>pim>if# exit
A: MV>config>router>pim# interface "mv-sfo"
A: MV>config>router>pim>if# exit
A: MV>config>router>pim# interface "mv-vlc"
A: MV>config>router>pim>if# exit
A: MV>config>router>pim# interface "p3-ix"
A: MV>config>router>pim>if# exit
A: MV>config>router>pim# rp
A: MV>config>router>pim>rp# static
A: MV>config>router>pim>rp>static# address 2.22.187.237
A: MV>config>router>pim>rp>static>address# group-prefix 224.24.24.24/32
A: MV>config>router>pim>rp>static>address# exit
A: MV>config>router>pim>rp# static
A: MV>config>router>pim>rp# exit
A: MV>config>router>pim# info

--------------------------------------------
interface "system"
exit
interface "mv-sfo"
exit
interface "mv-vlc"
exit
interface "p3-ix"
exit
rp
static
    address 2.22.187.237
    group-prefix 224.24.24.24/32
exit
exit
bsr-candidate
    address 2.22.187.236
    no shutdown
exit
rp-candidate
    address 2.22.187.236
    no shutdown
exit
exit
--------------------------------------------
A: MV>config>router>pim#
Example:

```
A:SFO>config>router# pim
A:SFO>config>router>pim# interface "system"
A:SFO>config>router>pim>if# exit
A:SFO>config>router>pim# interface "sfo-sfc"
A:SFO>config>router>pim>if# exit
A:SFO>config>router>pim# interface "sfo-was"
A:SFO>config>router>pim>if# exit
A:SFO>config>router>pim# interface "sfo-mv"
A:SFO>config>router>pim>if# exit
A:SFO>config>router>pim# rp
A:SFO>config>router>pim>rp# static
A:SFO>config>router>pim>rp>static# address 2.22.187.237
A:SFO>config>router>pim>rp>static>address# group-prefix 224.24.24.24/32
A:SFO>config>router>pim>rp>static>address# exit
A:SFO>config>router>pim>rp# exit
A:SFO>config>router>pim# exit
A:SFO>config>router>pim# info
```

```
-------------------------------
interface "system"
 exit
interface "sfo-sjc"
 exit
interface "sfo-was"
 exit
interface "sfo-mv"
 exit
 rp
 static
 address 2.22.187.237
 group-prefix 224.24.24.24/32
 exit
exit
 bsr-candidate
 address 2.22.187.239
 no shutdown
 exit
 rp-candidate
 address 2.22.187.239
 no shutdown
 exit
 exit
-------------------------------
A:SFO>config>router>pim#
```
Example:
A:WAS>config>router# pim
A:WAS>config>router>pim# interface "system"
A:WAS>config>router>pim>if# exit
A:WAS>config>router>pim# interface "was-sfo"
A:WAS>config>router>pim>if# exit
A:WAS>config>router>pim# interface "was-vlc"
A:WAS>config>router>pim>if# exit
A:WAS>config>router>pim# interface "p4-ix"
A:WAS>config>router>pim>if# exit
A:WAS>config>router>pim# rp
A:WAS>config>router>pim>rp# static
A:WAS>config>router>pim>rp>static# address 2.22.187.237
A:WAS>config>router>pim>rp>static>address# group-prefix 224.24.24/32
A:WAS>config>router>pim>rp# exit
A:WAS>config>router>pim# info
---------------------------------------------------------------------
interface "system"
exit
interface "was-sfo"
exit
interface "was-vlc"
exit
interface "p4-ix"
exit
rp
static
    address 2.22.187.237
    group-prefix 224.24.24/32
    exit
exit
bsr-candidate
    address 2.22.187.240
    no shutdown
exit
rp-candidate
    address 2.22.187.240
    no shutdown
exit
exit
---------------------------------------------------------------------
A:WAS>config>router>pim#
Importing PIM Join/Register Policies

The import command provides a mechanism to control the (*,G) and (S,G) state that gets created on a router. Import policies are defined in the `config>router>policy-options` context.

Note, in the import policy, if an action is not specified in the entry then the default-action takes precedence. If no entry matches then the default-action also takes precedence. If no default-action is specified, then the default default-action is executed.

Use the following commands to configure PIM parameters:

**CLI Syntax:**
```
cfg-router# pim
    import {join-policy|register-policy} [policy-name]
        [.. policy-name]
```

The following example displays the command usage to apply the policy statement which does not allow join messages for group 229.50.50.208/32 and source 192.168.0.0/16 but allows join messages for 192.168.0.0/16, 229.50.50.208 (see Configuring Route Policy Components on page 730):

**Example:**
```
cfg-router# pim
cfg-router# pim import join-policy "foo"
cfg-router# pim no shutdown
```

The following example displays the PIM configuration:

```
A:LAX>cfg-router# pim info
-----------------------------------------------
import join-policy "foo"
interface "system"
exit
interface "lax-vls"
exit
interface "lax-sjc"
exit
interface "pl-ix"
exit
rp
static
    address 2.22.187.237
        group-prefix 224.24.24.24/3
    exit
    address 10.10.10.10
    exit
exit
bsr-candidate
shutdown
```
exit
rp-candidate
    shutdown
exit
exit
----------------------------------------------
A:LAX>config>router>pim#
Configuring Multicast Source Discovery Protocol (MSDP) Parameters

Use the following commands to configure basic MSDP parameters:

**CLI Syntax:**
```
config>router# msdp
   peer ip-address
      active-source-limit number
      authentication-key [authentication-key|hash-key]
      [hash|hash2]
      default-peer
      export policy-name [policy-name...(up to 5 max)]
      import policy-name [policy-name...(up to 5 max)]
      local-address ip-address
      receive-msdp-msg-rate number interval seconds [threshold threshold]
      no shutdown
      no shutdown
```

Use the following CLI syntax to configure MSDP parameters.

**Example:**
```
config>router>msdp# peer 10.20.1.1
config>router>msdp>peer# local-address 10.20.1.6
config>router>msdp>peer# no shutdown
config>router>msdp>peer# exit
config>router>msdp# no shutdown
config>router>msdp#
```

The following example displays the MSDP configuration:
```
ALA-48>config>router>msdp# info
-------------------------------------------
peer 10.20.1.1
   local-address 10.20.1.6
exit
-------------------------------------------
ALA-48>config>router>msdp#
```
Common Configuration Tasks

Configuring MCAC Parameters

The MCAC policies can be added to a SAP, spoke SDP, mesh SDP, an IGMP interface, and a PIM interface.

The following example displays the command usage to create MCAC policies.

**Example:**
```
config>router# mcac
config>router>mcac# policy "btv_fr"
config>router>mcac>policy# description "foreign TV offering"
config>router>mcac>policy# bundle "FOR" create
config>router>mcac>policy>bundle# bandwidth 30000
config>router>mcac>policy>bundle# channel 224.0.3.1 224.0.3.1 bw 4000
config>router>mcac>policy>bundle# channel 224.0.3.2 224.0.3.2 bw 4000
config>router>mcac>policy>bundle# channel 224.0.4.1 224.0.4.1 bw 3500 class high type mandatory
config>router>mcac>policy>bundle# channel 224.0.4.2 224.0.4.2 bw 3500 class high
config>router>mcac>policy>bundle# channel 224.0.4.3 224.0.4.3 bw 2800 type mandatory
config>router>mcac>policy>bundle# channel 224.0.4.4 224.0.4.4 bw 2800
config>router>mcac>policy>bundle# mc-constraints
config>router>mcac>policy>bundle>mc-constraints# level 1 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 2 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 3 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 4 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 5 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 6 bw 20000
config>router>mcac>policy>bundle>mc-constraints# lag-port-down 1 number-down 1 level 1
config>router>mcac>policy>bundle>mc-constraints# lag-port-down 1 number-down 2 level 3
config>router>mcac>policy>bundle>mc-constraints# lag-port-down 1 number-down 3 level 5
config>router>mcac>policy>bundle>mc-constraints# lag-port-down 2 number-down 1 level 1
config>router>mcac>policy>bundle>mc-constraints# lag-port-down 2 number-down 2 level 3
config>router>mcac>policy>bundle>mc-constraints# lag-port-down 2 number-down 3 level 5
config>router>mcac>policy>bundle>mc-constraints# exit
config>router>mcac>policy>bundle# no shutdown
config>router>mcac>policy>bundle# exit
config>router>mcac>policy# exit
config>router>mcac# policy "btv_vl"
config>router>mcac>policy# description "eastern TV offering"
config>router>mcac>policy# bundle "VRT" create
config>router>mcac>policy>bundle# bandwidth 120000
config>router>mcac>policy>bundle# channel 224.1.2.0 224.1.2.4 bw 4000 class high type mandatory
config>router>mcac>policy>bundle# channel 224.1.2.5 224.1.2.5 bw 20000 type mandatory
config>router>mcac>policy>bundle# channel 224.1.2.10 224.1.2.10 bw 8000 type mandatory
config>router>mcac>policy>bundle# channel 224.2.2.0 224.2.2.4 bw 4000
config>router>mcac>policy>bundle# channel 224.2.2.5 224.2.2.5 bw 10000 class high
config>router>mcac>policy>bundle# channel 224.2.2.6 224.2.2.6 bw 10000 class high
config>router>mcac>policy>bundle# channel 224.2.2.7 224.2.2.7 bw 10000
config>router>mcac>policy>bundle# channel 224.2.2.8 224.2.2.8 bw 10000
config>router>mcac>policy>bundle# mc-constraints
config>router>mcac>policy>bundle>mc-constraints# level 1 bw 60000
config>router>mcac>policy>bundle>mc-constraints# level 2 bw 50000
config>router>mcac>policy>bundle>mc-constraints# level 3 bw 40000
config>router>mcac>policy>bundle>mc-constraints# level 4 bw 30000
config>router>mcac>policy>bundle>mc-constraints# level 5 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 6 bw 10000
```
config>router>mac>policy>bundle>mc-constraints# lag-port-down 1 number-down 1 level 1
config>router>mac>policy>bundle>mc-constraints# lag-port-down 1 number-down 2 level 3
config>router>mac>policy>bundle>mc-constraints# lag-port-down 1 number-down 3 level 5
config>router>mac>policy>bundle>mc-constraints# lag-port-down 2 number-down 1 level 1
config>router>mac>policy>bundle>mc-constraints# lag-port-down 2 number-down 2 level 3
config>router>mac>policy>bundle>mc-constraints# lag-port-down 2 number-down 3 level 5
config>router>mac>policy>bundle>mc-constraints# exit
config>router>mac>policy>bundle# no shutdown
config>router>mac>policy>bundle# exit
config>router>mac>policy# exit

The following example displays the configuration:

*A:ALA-48>config>router>mcac# info
------------------------------------------------------------------
policy "btv_fr"
  description "foreign TV offering"
  bundle "FOR" create
    bandwidth 30000
    channel 224.0.3.1 224.0.3.1 bw 4000
class high type mandatory
    channel 224.0.3.2 224.0.3.2 bw 4000
    channel 224.0.4.1 224.0.4.1 bw 3500
    channel 224.0.4.2 224.0.4.2 bw 3500
    channel 224.0.4.3 224.0.4.3 bw 2800
class high type mandatory
    channel 224.0.4.4 224.0.4.4 bw 2800
  mc-constraints
    level 1 bw 20000
    level 2 bw 20000
    level 3 bw 20000
    level 4 bw 20000
    level 5 bw 20000
    level 6 bw 20000
    lag-port-down 1 number-down 1 level 1
    lag-port-down 1 number-down 2 level 3
    lag-port-down 1 number-down 3 level 5
    lag-port-down 2 number-down 1 level 1
    lag-port-down 2 number-down 2 level 3
    lag-port-down 2 number-down 3 level 5
  exit
  no shutdown
  exit
exit

policy "btv_vl"
  description "eastern TV offering"
  bundle "VRT" create
    bandwidth 120000
    channel 224.1.2.0 224.1.2.4 bw 4000
    channel 224.1.2.5 224.1.2.5 bw 20000
    channel 224.1.2.10 224.1.2.10 bw 8000
    channel 224.2.2.0 224.2.2.4 bw 4000
    channel 224.2.2.5 224.2.2.5 bw 10000
    channel 224.2.2.6 224.2.2.6 bw 10000
    channel 224.2.2.7 224.2.2.7 bw 10000
    channel 224.2.2.8 224.2.2.8 bw 10000
  mc-constraints
    level 1 bw 60000
    level 2 bw 50000
level 3 bw 40000
level 4 bw 30000
level 5 bw 20000
level 6 bw 10000
lag-port-down 1 number-down 1 level 1
lag-port-down 1 number-down 2 level 3
lag-port-down 1 number-down 3 level 5
lag-port-down 2 number-down 1 level 1
lag-port-down 2 number-down 2 level 3
lag-port-down 2 number-down 3 level 5
exit
no shutdown
exit
exit
------------------------------------------------------------------
*A:ALA-48>config>router>mcac#
Service Management Tasks

This section discusses the service management task to disable IGMP and PIM.

Disabling IGMP or PIM

Use the following CLI syntax to disable IGMP and PIM:

**CLI Syntax:**
```
config>router#
  igmp
  shutdown
msdp
  shutdown
pim
  shutdown
```

The following example displays the command usage to disable multicast:

**Example:**
```
config>router# igmp
config>router>igmp# shutdown
config>router>igmp# exit
config>router#
config>router>msdp# shutdown
config>router>msdp# exit
config>router# pim
config>router>pim# shutdown
config>router>pim# exit
```
The following example displays the configuration output:

```
A:LAX>config>router# info
----------------------------------------------
...                                          
#------------------------------------------
echo "IGMP Configuration"
#------------------------------------------
  igmp
    shutdown
    ssm-translate
      grp-range 229.255.0.1 231.2.2.2
      source 10.1.1.1
    exit
  exit
interface "lax-sjc"
  static
    group 230.1.1.1
  starg
  exit
  exit
interface "lax-vis"
  static
    group 229.255.0.2
    source 172.22.184.197
  exit
  exit
interface "p1-ix"
  exit
#------------------------------------------
  #--------------------------------------------------
  echo "MSDP Configuration"
  #--------------------------------------------------
  msdp
    shutdown
    peer 10.20.1.1
      local-address 10.20.1.6
    exit
    group "test"
      active-source-limit 50000
      receive-msdp-msg-rate 100 interval 300 threshold 5000
      export "LDP-export"
      import "LDP-import"
      local-address 10.10.10.103
      mode mesh-group
    peer 10.10.10.104
    exit
  exit
  #------------------------------------------
  #--------------------------------------------------
  echo "PIM Configuration"
  #--------------------------------------------------
  pim
```

shutdown
import join-policy "foo"
interface "system"
exit
interface "lax-sjc"
exit
interface "lax-vls"
exit
interface "p1-ix"
exit
rp
  static
    address 2.22.187.237
    group-prefix 224.24.24.24/32
    exit
    address 10.10.10.10
    exit
    exit
    bsr-candidate
    shutdown
    exit
    rp-candidate
    shutdown
    exit
exit
exit
#------------------------------------------
....
------------------------------------------
A:LAX>config>router#
Multicast Command Reference

Command Hierarchies

- Configuration Commands on page 85
  - IGMP Commands on page 85
  - PIM Commands on page 87
  - MSDP Commands on page 90
  - Multicast CAC Policy Commands on page 92
- Operational Commands on page 94
- Show Commands on page 94
- Clear Commands on page 95
- Debug Commands on page 97

Configuration Commands

```plaintext
config
  router
    [no] ip-fast-reroute
    [no] mc-maximum-routes number [log-only] [threshold threshold]
    [no] mc-maximum-routes
    multicast-info policy-name
    [no] multicast-info
```

IGMP Commands

```plaintext
config
  router
    [no] igmp
      [no] group-interface ip-int-name
        [no] disable-router-alert-check
        import policy-name
        [no] import
        max-groups value
        [no] max-groups
        max-grp-sources [1..1000]
        [no] max-grp-sources
        max-sources [1..1000]
        [no] max-sources
        mcac
          mc-constraints
            [no] shutdown
            policy policy-name
            [no] policy
            unconstrained-bw bandwidth mandatory-bw mandatory-bw
            [no] unconstrained-bw
```
--- [no] import
--- [no] sub-hosts-only
--- [no] subnet-check
--- version version
--- no version
--- [no] interface ip-int-name
--- [no] disable-router-alert-check
--- [no] group-interface ip-int-name
--- [no] shutdown
--- import policy-name
--- no import
--- max-groups value
--- no max-groups
--- mcac
--- mc-constraints
--- level level-id bw bandwidth
--- [no] level level-id
--- number-down number-lag-port-down level level-id
--- [no] number-down number-lag-port-down
--- [no] shutdown
--- policy mcac-policy-name
--- [no] policy
--- unconstrained-bw bandwidth mandatory-bw mandatory-bw
--- no unconstrained-bw
--- [no] shutdown
--- ssm-translate
--- [no] grp-range start end
--- [no] source ip-address
--- static
--- [no] group grp-ip-address
--- [no] source ip-address
--- [no] starg
--- [no] subnet-check
--- version version
--- no version
--- query-interval seconds
--- [no] query-interval
--- query-last-member-interval seconds
--- [no] query-last-member-interval
--- query-response-interval seconds
--- [no] query-response-interval
--- robust-count robust-count
--- [no] robust-count
--- [no] shutdown
--- ssm-translate
--- [no] grp-range start end
--- [no] source ip-address
--- [no] sub-hosts-only
--- [no] tunnel-interface rsvp-p2mp lsp-name
--- static
--- [no] group grp-ip-address
--- [no] source ip-address
--- [no] starg
PIM Commands

```
config
  router
    [no] pim
      apply-to {ies | non-ies | all | none}
      [no] enable-mdt-spt
      import {join-policy | register-policy} policy-name [, policy-name]
    [no] import {join-policy | register-policy}
    interface ip-int-name
      [no] assert-period assert-period
      [no] assert-period
      [no] bfd-enable [ipv4 | ipv6]
      [no] bsm-check-rtr-alert
      hello-interval hello-interval
      [no] hello-interval
      [no] hello-multiplier deci-units
      [no] hello-multiplier
      [no] improved-assert
      [no] ipv4-multicast-disable
      [no] ipv6-multicast-disable
      max-groups value
      [no] max-groups
      mcac
        mc-constraints
          [no] level level bw bandwidth
          [no] level level
          [no] number-down number-lag-port-down level level-id
          [no] number-down number-lag-port-down
          [no] shutdown
        policy policy-name
        [no] policy
        unconstrained-bw bandwidth mandatory-bw mandatory-bw
        [no] unconstrained-bw
        multicast-senders {auto | always | never}
        [no] multicast-senders
        priority dr-priority
        [no] priority
        [no] shutdown
        sticky-dr [priority dr-priority]
        [no] sticky-dr
        three-way-hello [compatibility-mode]
        [no] three-way-hello
        [no] tracking-support
        [no] ipv4-multicast-disable
        ipv6-multicast-disable
        [no] lag-usage-optimization
        [no] mc-ecmp-balance
        mc-ecmp-balance-hold minutes
        [no] mc-ecmp-balance-hold
        [no] mc-ecmp-hashing-enabled
        [no] non-dr-attract-traffic
        rp
          [no] anycast rp-ip-address
          [no] rp-set-peer ip-address
```
— [no] auto-rp-discovery
— bootstrap-export policy-name [.. policy-name]
— no bootstrap-export
— bootstrap-import policy-name [.. policy-name]
— no bootstrap-import
— bsr-candidate
  — address ip-address
  — no address
  — hash-mask-len hash-mask-length
  — no hash-mask-len
  — priority bootstrap-priority
  — no priority
  — [no] shutdown
— ipv6
  — [no] anycast rp-ip-address
    — [no] rp-set-peer ip-address
  — bsr-candidate
    — address ip-address
    — no address
    — hash-mask-len hash-mask-length
    — no hash-mask-len
    — priority bootstrap-priority
    — no priority
    — [no] shutdown
— [no] embedded-rp
  — [no] group-range ipv6-address/prefix-length
  — [no] shutdown
— rp-candidate
  — address ip-address
  — no address
  — [no] group-range {grp-ip-address/mask | grp-ip-address netmask}
    — holdtime holdtime
    — no holdtime
    — priority priority
    — no priority
    — [no] shutdown
— static
  — [no] address ip-address
    —[no] group-prefix {grp-ip-address/mask | grp-ip-address netmask}
    —[no] override
— rp-candidate
  — address ip-address
  — no address
  — [no] group-range {grp-ip-address/mask | grp-ip-address netmask}
    — holdtime holdtime
    — no holdtime
    — priority priority
    — no priority
    — [no] shutdown
— static
  — [no] address ip-address
Multicast

— [no] **group-prefix** \{grp-ip-address/mask | grp-ip-address netmask\}
— [no] override
— [no] rp6-table \{rtable6-m | rtable6-u | both\}
— [no] shutdown
— spt-switchover-threshold \{grp-ip-address/mask | grp-ip-address netmask\} spt-threshold
— no spt-switchover-threshold \{grp-ip-address/mask | grp-ip-address netmask\}
— [no] ssm-groups
— [no] group-range \{ip-prefix/mask | ip-prefix netmask\}
— [no] tunnel-interface \{rsvp-p2mp lsp-name | ldp-p2mp p2mp-id\} [sender ip-address]
MSDP Commands

```
config
    — router
        — [no] msdp
            — [no] active-source-limit number
            — [no] data-encapsulation
            — export [policy-name...(up to 5 max)]
            — no export
            — [no] group group-name
                — [no] active-source-limit number
                — export policy-name [policy-name...(up to 5 max)]
                — no export
                — import policy-name [policy-name...(up to 5 max)]
                — no import
                — local-address address
                — no local-address
                — mode {mesh-group | standard}
            — [no] peer peer-address
                — [no] active-source-limit number
                — authentication-key [authentication-key | hash-key]
                    [hash | hash2]
                — no authentication-key
                — [no] default-peer
                — export policy-name [policy-name...(up to 5 max)]
                — no export
                — import policy-name [policy-name...(up to 5 max)]
                — no import
                — local-address address
                — no local-address
                — [no] shutdown
            — receive-msdp-msg-rate number interval seconds [threshold number]
            — no receive-msdp-msg-rate
            — [no] shutdown
            — import policy-name [policy-name...(up to 5 max)]
            — no import
            — local-address address
            — no local-address
            — [no] peer peer-address
                — [no] active-source-limit number
                — authentication-key [authentication-key | hash-key]
                    [hash | hash2]
                — no authentication-key
                — [no] default-peer
                — export policy-name [policy-name...(up to 5 max)]
                — no export
                — import policy-name [policy-name...(up to 5 max)]
                — no import
                — local-address address
                — no local-address
                — receive-msdp-msg-rate number interval seconds [threshold number]
                — no receive-msdp-msg-rate
                — [no] shutdown
            — receive-msdp-msg-rate number interval seconds [threshold number]
            — no receive-msdp-msg-rate
            — rpf6-table {rtable-m | rtable-u | both}
```
— no rpf6-table
— sa-timeout seconds
— no sa-timeout
— [no] shutdown
— [no] source prefix/mask
  — active-source-limit number
  — no active-source-limit number
Multicast CAC Policy Commands

```plaintext
config
  - [no] router
  - mcac
    - [no] policy policy-name
    - [no] bundle bundle-name
    - bandwidth bandwidth
    - no bandwidth
    - channel start-address end-address bw bandwidth [class {high | low}] [type {mandatory | optional}]
    - no channel mc-ip-addr mc-ip-addr
    - description description-string
    - no description
    - mc-constraints
      - lag-port-down lag-id number-down number-lag-port-down level level-id
      - no lag-port-down lag-id number-down number-lag-port-down
      - level level bw bandwidth
      - no level level
    - [no] shutdown
    - default-action {accept | discard}
    - description description-string
    - no description
```
Multicast Listener Discovery (MLD) Commands

```plaintext
config
  — [no] router
    — [no] mld
      — [no] interface ip-int-name
        — [no] disable-router-alert-check
        — import policy-name
        — no import
        — max-groups value
        — no max-groups
        — query-interval seconds
        — no query-interval
        — query-last-member-interval seconds
        — no query-last-member-interval
        — query-response-interval seconds
        — no query-response-interval
        — [no] shutdown
        — static
          — [no] group grp-ipv6-address
            — [no] source src-ipv6-address
            — [no] starg
          — version version
          — no version
        — query-interval seconds
        — no query-interval
        — query-last-member-interval seconds
        — no query-last-member-interval
        — query-response-interval seconds
        — no query-response-interval
        — robust-count robust-count
        — no robust-count
        — [no] shutdown
        — ssm-translate
          — [no] grp-range start end
            — [no] source src-ipv6-address
```
Operational Commands

- mrinfo ip-address [router router-name | service]
- mstat source ip-address [group grp-ip-address] [destination dst-ip-address] [hop hop] [router router-name | service] [wait-time wait-time]
- mtrace source ip-address [group grp-ip-address] [destination dst-ip-address] [hop hop] [router router-name | service] [wait-time wait-time]

Show Commands

show
- router
  - igmp
    - group [grp-ip-address]
    - group summary
    - hosts [group grp-address] [detail] [fwd-service service-id] [grp-interface ip-int-name]
    - hosts [host ip-address] [group grp-address] [detail]
    - hosts summary
    - interface [ip-int-name | ip-address] [group grp-address] [detail]
    - ssm-translate
      - ssm-translate interface interface-name
    - static [ip-int-name | ip-addr]
    - statistics [ip-int-name | ip-address]
    - statistics host [ip-address]
    - status

show
- router
  - pim
    - anycast [detail]
    - crp [ip-address]
    - s-pmsi [data-mt-interface-name] [detail]
    - group [grp-ip-address] [source ip-address] [type {startrp|starg|sg}] [detail] [family]
    - interface [ip-int-name | mt-int-name | ip-address] [group grp-ip-address] source ip-address] [type {startrp|starg|sg}] [detail] [family]
    - neighbor [ip-address | ip-int-name [address ip-address]] [detail] [family]
    - rp [ip-address]
    - rp-hash grp-ip-address
    - statistics [ip-int-name | mt-int-name | ip-address] [family]
    - status [detail] [family]

show
- router
  - mld
    - group [grp-ipv6-address]
    - interface [ip-int-name | ip-address] [group] [grp-ipv6-address] [detail]
    - ssm-translate
    - static [ip-int-name | ip-address]
    - statistics [ip-int-name | ipv6-address]
    - status
Multicast

---

msdp

- **group** [group-name] [detail]
- **peer** [ip-address] [group group-name] [detail]
- **source** [ip-address/mask] [type {configured | dynamic | both}] [detail]
- **source-active** [group ip-address] [local] [originator ip-address] [peer ip-address] [source ip-address] [group ip-address source ip-address] [detail]
- **source-active-rejected** [peer-group name] [group ip-address] [source ip-address] [originator ip-address] [peer ip-address]
- **statistics** [peer ip-address]
- **status**

---

mcac

- **policy** [policy-name [bundle bundle-name]] [protocol protocol-name] [interface if-name] [detail]
- **statistics**

---

show

- **router** {router-instance}

---

mvpn

---

show

- **router**
  - **tunnel-table** [ip-address [mask]] [protocol | sdp sdp-id]
  - **tunnel-table** [summary]

---

Clear Commands

clear

- **router**
  - **igmp**
    - **database** [interface ip-int-name|ip-address] group grp-ip-address [source src-ip-address]
    - **database** grp-interface interface-name [fwd-service service-id]
    - **database** [interface ip-int-name|ip-address] group grp-ip-address source src-ip-address
    - **database** host [ip-address]
    - **database** interface ip-int-name|ip-address [group grp-ip-address] [source src-ip-address]
    - **statistics** [interface ip-int-name | ip-address]
    - **version** [interface ip-int-name | ip-address]
  - **mld**
    - **database** [interface ip-int-name|ipv6-address] [group ip-address] [source ip-address]
    - **statistics** [ip-int-name|ipv6-address]
    - **version** [ip-int-name | ip-address]
  - **msdp**
    - **cache** [peer ip-address] [group ip-address] [source ip-address] [originrp ip-address]
    - **statistics** [peer ip-address]
  - **pim**
    - **database** [interface ip-int-name | ip-address | mt-int-name] [group grp-ip-address] [source ip-address] [family]
    - **neighbor** [interface ip-int-name | ip-address] [family]
    - **s-pmsi** [mdSrcAddr] [mdGrpAddr] [vprnSrcAddr vprnGrpAddr]
clear
  — service
    — id
      — igmp-snooping
        — port-db sap sap-id [group grp-address [source ip-address]]
        — port-db sdp sdp-id:vc-id [groupgrp-address [source ip-address]]
        — querier
        — statistics [all | sap sap-id | sdp sdp-id:vc-id]
      — pim-snooping
        — database [[sap sap-id | sdp sdp-id:vc-id] [group grp-ip-address] [source src-ip-address]]
        — neighbor [ip-address | sap sap-id | sdp sdp-id:vc-id]
        — statistics [sap sap-id | sdp sdp-id:vc-id]
Debug Commands

debug
  — router
    — igmp
      — [no] group-interface [fwd-service service-id] [ip-int-name]
      — host [ip-address]
      — host [fwd-service service-id] group-interface ip-int-name
      — no host [ip-address]
      — no host [fwd-service service-id] group-interface ip-int-name
      — [no] interface [ip-int-name | ip-address]
      — mcs [ip-int-name]
      — no mcs
      — packet [query | v1-report | v2-report | v3-report | v2-leave] host ip-address
      — no packet [query | v1-report | v2-report | v3-report | v2-leave] [ip-int-name | ip-address]

  — [no] msdp
    — packet [pkt-type] peer ip-address
    — no packet
- `pim [grp-address]`
- `no pim`
- `rtm [rp-address]`
- `no rtm`
- `sa-db [group grpAddr] [source srcAddr] [rp rpAddr]`
- `no sa-db`
Configuration Commands

Generic Commands

shutdown

Syntax  [no] shutdown

Context  config>router>igmp
config>router>igmp>interface
config>router>igmp>interface>group-interface
config>router>igmp>if>mcac>mc-constraints
config>router>pim
config>router>pim>interface
config>router>pim>rp>rp-candidate
config>router>pim>rp>bsr-candidate
config>router>pim>rp>ipv6>rp-candidate
config>router>pim>rp>ipv6>bsr-candidate
config>router>pim>if>mcac>mc-constraints
config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>mcac>policy>bundle
config>router>mld
config>router>mld>interface

Description  The shutdown command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command.

The shutdown command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system generated configuration files.

The no form of the command puts an entity into the administratively enabled state.

Default  no shutdown:  config>router>igmp
config>router>igmp>interface ip-int-name
config>router>pim
config>router>pim>rp>rp-candidate

shutdown: config>router>pim>rp>bsr-candidate
Multicast Commands

ssm-translate

Syntax  ssm-translate
Context  config>router>igmp>interface>shutdown
Description  This command adds or removes ssm-translate group ranges.

source

Syntax  [no] source ip-address
Context  config>router>igmp>interface>shutdown>ssm-translate>grp-range
Description  This command adds or removes source addresses for the SSM translate group range.
Parameters  ip-address — a.b.c.d - unicast source address

grp-range

Syntax  [no] grp-range start end
Context  config>router>igmp>interface>shutdown>ssm-translate
Description  This command adds or removes SSM translate group range entries.
Parameters  start — a.b.c.d - multicast group range start address
            end — a.b.c.d - multicast group range end address

description

Syntax  description description-string
        no description
Context  config>router>mcac>policy
            config>router>mcac>policy>bundle
Description  This command creates a text description stored in the configuration file for a configuration context.
             The description command associates a text string with a configuration context to help identify the context in the configuration file.
             The no form of the command removes any description string from the context.
Multicast

Default
No description associated with the configuration context.

Parameters
string — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-fast-reroute

Syntax [no] ip-fast-reroute

Context config>router

Description This command configures IP fast reroute.

mc-maximum-routes

Syntax mc-maximum-routes number [log-only] [threshold threshold]
no mc-maximum-routes

Context config>router

Description This command specifies the maximum number of multicast routes that can be held within a VPN routing/forwarding (VRF) context. When this limit is reached, a log and SNMP trap are sent. If the log-only parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then no new joins will be processed.

The no form of the command disables the limit of multicast routes within a VRF context. Issue the no form of the command only when the VPRN instance is shutdown.

Default no mc-maximum-routes

Parameters number — Specifies the maximum number of routes to be held in a VRF context.

Values 1 — 2147483647

log-only — Specifies that if the maximum limit is reached, only log the event. log-only does not disable the learning of new routes.

threshold threshold — The percentage at which a warning log message and SNMP trap should be sent.

Values 0 — 100

Default 1
multicast-info

Syntax  multicast-info-policy *policy-name*
        no multicast-info-policy

Context  configure>router

Description  This command configures multicast information policy.

Parameters  *policy-name* — Specifies the policy name.

Values  32 chars max
**Router IGMP Commands**

**igmp**

**Syntax**  
[no] igmp

**Context**  
config>router

**Description**  
This command enables the Internet Group Management Protocol (IGMP) context. When the context is created, the IGMP protocol is enabled.

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to neighboring multicast routers. An IP multicast router can be a member of one or more multicast groups, in which case it performs both the “multicast router part” of the protocol which collects the membership information needed by its multicast routing protocol, and the “group member part” of the protocol which informs itself and other neighboring multicast routers of its memberships.

The **no** form of the command disables the IGMP instance. To start or suspend execution of IGMP without affecting the configuration, use the **no shutdown** command.

**Default**  
none

**interface**

**Syntax**  
[no] interface ip-int-name

**Context**  
config>router>igmp

**Description**  
This command enables the context to configure an IGMP interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled.

The **no** form of the command deletes the IGMP interface. The **shutdown** command in the **config>router>igmp>interface** context can be used to disable an interface without removing the configuration for the interface.

**Default**  
**no interface** — No interfaces are defined.

**Parameters**  
*ip-int-name* — The IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.
disable-router-alert-check

**Syntax**

```plaintext
[no] disable-router-alert-check
```

**Context**

```plaintext
config>router>igmp>if
config>router>igmp>group-interface
```

**Description**

This command enables the router alert checking for IGMP messages received on this interface. The `no` form of the command disables the IGMP router alert check option.

group-interface

**Syntax**

```plaintext
[no] group-interface ip-int-name
```

**Context**

```plaintext
config>router>igmp>if
```

**Description**

This command enables IGMP on a group-interface in a VRF context. Activating IGMP under the group-interface is a prerequisite for subscriber replication. The group-interface is also needed so that mcac can be applied and various IGMP parameters defined.

This command can be used in a regular, wholesaler or retailer type of VRF. Note that the retailer VRF does not have the concept of group-interfaces under the subscriber-interface hierarchy. In case that this command is applied to a retailer VRF instance, the optional fwd-service command must be configured. The fwd-service command is referencing the wholesaler VRF in which the traffic is ultimately replicated. Note that redirection in the retailer VRF is supported.

This command enables IGMP on a group-interface in the Global Routing Table (GRT). The group-interface in GRT is defined under the IES service. Activating IGMP under the group-interface is a prerequisite for subscriber replication. The group-interface is also needed so that MCAC can be applied and various IGMP parameters defined.

**Default**

none

**Parameters**

`ip-int-name` — Specifies the name of the group interface.

import

**Syntax**

```plaintext
import policy-name
no import
```

**Context**

```plaintext
configure>router>igmp>interface
configure>router>igmp>group-interface
configure>service>vprn>igmp>interface
configure>service>vprn>igmp>group-interface
configure>subscr-mgmt>igmp-policy
```

**Description**

This command applies the referenced IGMP policy (filter) to a subscriber or a group-interface. An IGMP filter is also known as a black/white list and it is defined under the `configure>router>policy-options`. 
When redirection is applied, only the import policy from the subscriber will be in effect. The import policy under the group interface is applicable only for IGMP states received directly on the sap (AN in IGMP proxy mode).

The no form of the command removes the policy association from the IGMP instance.

Default: no import — No import policy specified.

Parameters:
- policy-name — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the config>router>policy-options context.

sub-hosts-only

Syntax: [no] sub-hosts-only
Context: config>router>igmp>group-interface>mcac
Description: This command enables the handling of IGMP joins received from hosts that are not known in subscriber management or on which no IGMP policy is applied.

The no form of the command disables the command.

Default: sub-hosts-only

sub-hosts-only

Syntax: [no] sub-hosts-only
Context: config>router>igmp>group-interface
Description: This command disables processing of IGMP messages outside of the subscriber-host context. No other hosts outside of the subscriber-hosts can create IGMP states.

Disabling this command will allow creation of the IGMP states that correspond to the AN that operate in IGMP proxy mode. In this mode the AN will hide source IP addresses of IGMP messages and will source IGMP messages with its own IP address. In this case an IGMP state can be created under the sap context. This IGMP state creation under the sap is controlled via the import policy under the group-interface.

IGMP state processing for regular subscriber-hosts is unaffected by this command.

The no form of the command disables the command.

Default: sub-hosts-only
max-groups

Syntax

max-groups value
no max-groups

Context
config>router>igmp>if
config>router>igmp>group-interface
config>router>pim>if

Description
This command specifies the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed. This command is applicable for IPv4 and IPv6.

Default
0, no limit to the number of groups.

Parameters

value — Specifies the maximum number of groups for this interface.

Values
1 — 16000

max-grp-sources

Syntax

max-grp-sources [1..1000]
no max-grp-sources

Context
config>router>igmp>group-interface

max-sources

Syntax

max-sources [1..1000]
no max-sources

Context
config>router>igmp>group-interface

static

Syntax

static

Context
config>router>igmp>if

Description
This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Default
none
group

Syntax  [no] group grp-ip-address

Context  config>router>igmp>if>static

Description  This command enables the context to add a static multicast group either as a (*,G) or one or more (S,G) records. Use IGMP static group memberships to test multicast forwarding without a receiver host. When IGMP static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static IGMP group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static IGMP group entries do not generate join messages toward the RP.

Default  none

Parameters  
- grp-ip-address — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group.

source

Syntax  [no] source ip-address

Context  config>router>igmp>if>static>group
config>router>igmp>ssm-translate>grp-range

Description  This command specifies a IPv4 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the source(s) that the traffic is expected.

The source command is mutually exclusive with the specification of individual sources for the same group.

The source command in combination with the group is used to create a specific (S,G) static group entry.

Use the no form of the command to remove the source from the configuration.

Default  none

Parameters  
- ip-address — Specifies the IPv4 unicast address.

starg

Syntax  [no] starg

Context  config>router>igmp>if>static>group

Description  This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the no form of the command to remove the starg entry from the configuration.

Default  none
subnet-check

Syntax [no] subnet-check

Context config>router>igmp>interface
        config>router>igmp>group-interface>mcac

Description This command enables subnet checking for IGMP messages received on this interface. All IGMP packets with a source address that is not in the local subnet are dropped.

Default enabled

version

Syntax version version
        no version

Context config>router>igmp>interface
        config>router>igmp>group-interface>mcac

Description This command specifies the IGMP version. If routers run different versions of IGMP, they will negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version. For IGMP to function correctly, all routers on a LAN should be configured to run the same version of IGMP on that LAN.

For IGMPv3, note that a multicast router that is also a group member performs both parts of IGMPv3, receiving and responding to its own IGMP message transmissions as well as those of its neighbors.

Default 3

Parameters version — Specifies the IGMP version number.

Values 1, 2, 3

query-interval

Syntax query-interval seconds
        no query-interval

Context config>router>igmp

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default 125

seconds — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 — 1024
query-last-member-interval

Syntax  query-last-member-interval seconds

Context  config>router>igmp

Description  This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default  1

Parameters  seconds — Specifies the frequency, in seconds, at which query messages are sent.

   Values  1 — 1024

query-response-interval

Syntax  query-response-interval seconds

Context  config>router>igmp

Description  This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default  10

Parameters  seconds — Specifies the length of time to wait to receive a response to the host-query message from the host.

   Values  1 — 1023

robust-count

Syntax  robust-count robust-count
       no robust-count

Context  config>router>igmp

Description  This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default  2

Parameters  robust-count — Specify the robust count value.

   Values  2 — 10
ssm-translate

Syntax  ssm-translate
Context  config>router>igmp

Description  This command enables the context to configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the source command with starg command enabled.

grp-range

Syntax  [no] grp-range start end
Context  config>router>igmp>ssm-translate

Description  This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters  
  start — An IP address that specifies the start of the group range.
  end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the start value.

source

Syntax  [no] source ip-address
Context  config>router>igmp>ssm-translate>grp-range

Description  This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by grp-range start and end parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters  ip-address — Specifies the IP address that will be sending data.

tunnel-interface

Syntax  [no] tunnel-interface rsvp-p2mp lsp-name
Context  config>router>pim
 config>router>igmp

Description  This command creates a tunnel interface associated with an RSVP P2MP LSP. IPv4 multicast packets are forwarded over the P2MP LSP at the ingress LER based on a static join configuration of the multicast group against the tunnel interface associated with the originating P2MP LSP. At the egress LER, packets of a
multicast group are received from the P2MP LSP via a static assignment of the specific <S,G> to the tunnel interface associated with a terminating LSP.

At ingress LER, the tunnel interface identifier consists of a string of characters representing the LSP name for the RSVP P2MP LSP. The user can create one or more tunnel interfaces in PIM and associate each to a different RSVP P2MP LSP. P2mp-ID is required to configure LDP P2MP LSP tunnel interfaces. Sender address for a tunnel interface must be specified only on the leaf node.

At egress LER, the tunnel interface identifier consists of a couple of string of characters representing the LSP name for the RSVP P2MP LSP followed by the system address of the ingress LER. The LSP name must correspond to a P2MP LSP name configured by the user at the ingress LER. The LSP name string must not contain "::" (two ::s) nor contain a "::" (single ::) at the end of the LSP name. However, a "::" (single ::) can appear anywhere in the string except at the end of the name.

Default none

Parameters

rsvp-p2mp lsp-name — Specifies the LSP. The LSP name can be up to 32 characters long and must be unique.

psmp-id — Identifier used for signaling mLDP P2MP LSP.

Values 14294967296

static

Syntax static

Context config>router>igmp>tunnel-interface

Description This command provides the context to configure static multicast receiver hosts on a tunnel interface associated with an RSVP P2MP LSP.

When enabled, data is forwarded to an interface without receiving membership reports from host members.

Default none

group

Syntax [no] group grp-ip-address

Context config>router>igmp>tunnel-interface>static

Description This command enables the context to add a static multicast group either as a (*,G) or one or more (S,G) records.

The user can assign static multicast group joins to a tunnel interface associated with an RSVP P2MP LSP. Note that a given <*,G> or <S,G> can only be associated with a single tunnel interface.

A multicast packet which is received on an interface and which succeeds the RPF check for the source address will be replicated and forwarded to all OIFs which correspond to the branches of the P2MP LSP. The packet is sent on each OIF with the label stack indicated in the NHLFE of this OIF. The packets
also be replicated and forwarded natively on all OIFs which have received IGMP or PIM joins for this <S,G>.

The multicast packet can be received over a PIM or IGMP interface which can be an IES interface, a spoke SDP terminated IES interface, or a network interface.

**Default**
none

**Parameters**

*grp-ip-address* — Specifies a multicast group address that receives data on a tunnel interface. The IP address must be unique for each static group.

---

**source**

**Syntax**

```plaintext
[no] source ip-address
```

**Context**

`config>router>igmp>tunnel-interface>static>group`

**Description**

This command specifies a IPv4 unicast address of a multicast source. The source command is mutually exclusive with the specification of individual sources for the same group. The source command in combination with the group is used to create a specific (S,G) group entry in a static group join on a tunnel interface associated with a P2MP RSVP LSP.

The `no` form of the command removes the source from the configuration.

**Default**
none

**Parameters**

*ip-address* — Specifies the IPv4 unicast address.

---

**starg**

**Syntax**

```plaintext
[no] starg
```

**Context**

`config>router>igmp>tunnel-interface>static>group`

**Description**

This command adds a static (*,G) group entry in a static group join on a tunnel interface associated with a P2MP RSVP LSP.

This command can only be enabled if no existing source addresses for this group are specified.

The `no` form of the command removes the starg entry from the configuration.

**Default**
none
**Router PIM Commands**

**pim**

**Syntax**  
[no] pim

**Context**  
config>router

**Description**  
This command configures a Protocol Independent Multicast (PIM) instance.

PIM is used for multicast routing within the network. Devices in the network can receive the multicast feed requested and non-participating routers can be pruned. The router OS supports PIM sparse mode (PIM-SM).

**Default**  
not enabled

**interface**

**Parameters**  
[no] interface ip-int-name

**Context**  
config>router>pim

**Description**  
This command creates a logical IP routing interface.

Interface names are case-sensitive and must be unique within the group of defined IP interfaces defined for config router interface and config services interface. Interface names must not be in the dotted decimal notation of an IP address. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either the interface names or the IP addresses. Ambiguity can exist if an IP address is used as an IP address and an interface name. Duplicate interface names can exist in different router instances, although this is not recommended because it is confusing.

The no form of the command removes the IP interface and all the associated configurations.

**Default**  
No interfaces or names are defined within PIM.

**Parameters**  
ip-int-name — The name of the IP interface. Interface names must be unique within the group of defined IP interfaces for config router interface and config services interface commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

**Values**  
1 — 32 alphanumeric characters.

If the ip-int-name already exists, the context is changed to maintain that IP interface. If ip-int-name does not exist, the interface is created and the context is changed to that interface for further command processing.
apply-to

Syntax  apply-to {ies | non-ies | all | none}

Context  config>router>pim

Description  This command creates a PIM interface with default parameters.

If a manually created or modified interface is deleted, the interface will be recreated when (re)processing the apply-to command and if PIM is not required on a specific interface a shutdown should be executed.

The apply-to command is first saved in the PIM configuration structure. Then, all subsequent commands either create new structures or modify the defaults as created by the apply-to command.

Default  none (keyword)

Parameters  ies — Creates all IES interfaces in PIM.
            non-ies — Non-IES interfaces are created in PIM.
            all — All IES and non-IES interfaces are created in PIM.
            none — Removes all interfaces that are not manually created or modified. It also removes explicit no interface commands if present.

assert-period

Syntax  assert-period assert-period
        no assert-period

Context  config>router>pim>if

Description  This command configures the period for periodic refreshes of PIM Assert messages on an interface.

The no form of the command removes the assert-period from the configuration.

Default  no assert-period

Parameters  assert-period — Specifies the period for periodic refreshes of PIM Assert messages on an interface.
            Values  1 — 300 seconds

bfd-enable

Parameters  [no] bfd-enable [ipv4 | ipv6]

Context  config>router>pim>interface

Description  This command enables the use of IPv4 or IPv6 bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.
The no form of this command removes BFD from the associated IGP protocol adjacency.

**Default**  

no bfd-enable

### enable-mdt-spt

**Syntax**  

[no] enable-mdt-spt

**Context**  

config>router>pim

**Description**  

This command is used to enable SPT switchover for default MDT. On enable, PIM instance resets all MDTs and reinitiate setup.

The no form of the command disables SPT switchover for default MDT. On disable, PIM instance resets all MDTs and reinitiate setup.

**Default**  

no enable-mdt-spt

### import

**Syntax**  

import {join-policy | register-policy} [policy-name [. . policy-name]]  

no import {join-policy | register-policy}

**Context**  

config>router>pim

**Description**  

This command specifies the import route policy to be used. Route policies are configured in the config>router>policy-options context.

When an import policy is not specified, BGP routes are accepted by default. Up to five import policy names can be specified.

The no form of the command removes the policy association from the instance.

**Default**  

no import join-policy  

no import register-policy

**Parameters**  

- **join-policy** — Use this command to filter PIM join messages which prevents unwanted multicast streams from traversing the network.

- **register-policy** — This keyword filters register messages. PIM register filters prevent register messages from being processed by the RP. This filter can only be defined on an RP. When a match is found, the RP immediately sends back a register-stop message.

- **policy-name** — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the config>router>policy-options context.
ipv4-multicast-disable

Syntax  

`[no] ipv4-multicast-disable`

Context  

`configure>router>pim`

`configure>router>pim>interface`

Description  

This command administratively disables/enables PIM operation for IPv4.

Default  

no ipv4-multicast-disable

lag-usage-optimization

Syntax  

`[no] lag-usage-optimization`

Context  

`configure>router>pim`

Description  

This command specifies whether the router should optimize usage of the LAG such that traffic for a given multicast stream destined to an IP interface using the LAG is sent only to the forwarding complex that owns the LAG link on which it will actually be forwarded.

Changing the value causes the PIM protocol to be restarted.

If this optimization is disabled, the traffic will be sent to all the forwarding complexes that own at least one link in the LAG.

Note that changes made for 9G multicast hashing causes Layer 4 multicast traffic to not hashed. This is independent whether `lag-usage-optimization` is enabled or disabled.

mc-ecmp-balance

Syntax  

`[no] mc-ecmp-balance`

Context  

`configure>router>pim`

Description  

This command enables multicast balancing of traffic over ECMP links. When enabled, each multicast stream that needs to be forwarded over an ECMP link will be re-evaluated for the total multicast bandwidth utilization. Re-evaluation occurs on the ECMP interface in question.

The `no` form of the command disables the multicast balancing.

mc-ecmp-balance-hold

Syntax  

`mc-ecmp-balance-hold` `minutes`

`no mc-ecmp-balance-hold`

Context  

`configure>router>pim`

Description  

This command configures the hold time for multicast balancing over ECMP links.
Parameters

- **minutes** — Specifies the hold time, in minutes, that applies after an interface has been added to the ECMP link.

---

**mc-ecmp-hashing-enabled**

- **Syntax**
  
  
  - [no] mc-ecmp-hashing-enabled

- **Context**
  
  - configure>router>pim

- **Description**
  
  This command enables hash-based multicast balancing of traffic over ECMP links and causes PIM joins to be distributed over the multiple ECMP paths based on a hash of S and G (and possibly next-hop IP). When a link in the ECMP set is removed, the multicast streams that were using that link are redistributed over the remaining ECMP links using the same hash algorithm. When a link is added to the ECMP set new joins may be allocated to the new link based on the hash algorithm, but existing multicast streams using the other ECMP links stay on those links until they are pruned.

  Hash-based multicast balancing is supported for both IPv4 and IPv6.

  This command is mutually exclusive with the `mc-ecmp-balance` command in the same context.

  The `no` form of the command disables the hash-based multicast balancing of traffic over ECMP links.

- **Default**
  
  - no mc-ecmp-hashing-enabled

---

**ipv6-multicast-disable**

- **Syntax**
  
  - ipv6-multicast-disable

- **Context**
  
  - configure>router>pim
  
  - configure>router>pim>interface

- **Description**
  
  This command administratively disables/enables PIM operation for IPv6.

- **Default**
  
  - ipv6-multicast-disable

---

**bsm-check-rtr-alert**

- **Syntax**
  
  - [no] bsm-check-rtr-alert

- **Context**
  
  - config>router>pim>interface

- **Description**
  
  This command enables the checking of the router alert option in the bootstrap messages received on this interface.

- **Default**
  
  - no bsm-check-rtr-alert
hello-interval

**Syntax**
```
hello-interval hello-interval
no hello-interval
```

**Context**
```
config>router>pim>interface
```

**Description**
This command configures the frequency at which PIM Hello messages are transmitted on this interface. The `no` form of this command reverts to the default value of the hello-interval.

**Default**
30

**Parameters**
- `hello-interval` — Specifies the hello interval in seconds. A 0 (zero) value disables the sending of hello messages (the PIM neighbor will never timeout the adjacency).
  
  **Values**
  
  0 — 255 seconds

hello-multiplier

**Syntax**
```
hello-multiplier deci-units
no hello-multiplier
```

**Context**
```
config>router>pim>interface
```

**Description**
This command configures the multiplier to determine the holdtime for a PIM neighbor on this interface. The `hello-multiplier` in conjunction with the `hello-interval` determines the holdtime for a PIM neighbor.

**Parameters**
- `deci-units` — Specify the value, specified in multiples of 0.1, for the formula used to calculate the hello-holdtime based on the hello-multiplier:
  
  \[
  \text{hello-holdtime} = \frac{\text{hello-interval} \times \text{hello-multiplier}}{10}
  \]
  
  This allows the PIMv2 default timeout of 3.5 seconds to be supported.

  **Values**
  
  20 — 100

  **Default**
  35

improved-assert

**Syntax**
```
[no] improved-assert
```

**Context**
```
config>router>pim>interface
```

**Description**
The PIM assert process establishes a forwarder for a LAN and requires interaction between the control and forwarding planes. The assert process is started when data is received on an outgoing interface meaning that duplicate traffic is forwarded to the LAN until the forwarder is negotiated among the routers.

When the `improved-assert` command is enabled, the PIM assert process is done entirely in the control plane. The advantages are that it eliminates duplicate traffic forwarding to the LAN. It also improves performance since it removes the required interaction between the control and data planes.
NOTE: improved-assert is still fully interoperable with the draft-ietf-pim-sm-v2-new-xx, Protocol Independent Multicast - Sparse Mode (PIM-SM): Revised, and RFC 2362, Protocol Independent Multicast-Sparse Mode (PIM-SM), implementations. However, there may be conformance tests that may fail if the tests expect control-data plane interaction in determining the assert winner. Disabling the improved-assert command when performing conformance tests is recommended.

Default: enabled

### multicast-senders

**Syntax**
```
multicast-senders {auto | always | never}
no multicast-senders
```

**Context**
```
config>router>pim>interface
```

**Description**
This command configures how traffic from directly-attached multicast sources should be treated on broadcast interfaces. It can also be used to treat all traffic received on an interface as traffic coming from a directly-attached multicast source. This is particularly useful if a multicast source is connected to a point-to-point or unnumbered interface.

**Default**
auto

**Parameters**
- **auto** — Specifies that, on broadcast interfaces, the forwarding plane performs subnet-match check on multicast packets received on the interface to determine if the packet is from a directly-attached source. On unnumbered/point-to-point interfaces, all traffic is implicitly treated as coming from a remote source.

- **always** — Treats all traffic received on the interface as coming from a directly-attached multicast source.

- **never** — Specifies that, on broadcast interfaces, traffic from directly-attached multicast sources will not be forwarded. Note that traffic from a remote source will still be forwarded if there is a multicast state for it. On unnumbered/point-to-point interfaces, it means that all traffic received on that interface must not be forwarded.

### priority

**Syntax**
```
priority dr-priority
no priority
```

**Context**
```
config>router>pim>interface
```

**Description**
This command sets the priority value to elect the designated router (DR). The DR election priority is a 32-bit unsigned number and the numerically larger priority is always preferred.

The **no** form of the command restores the default values.

**Default**
1
Parameters

priority — Specifies the priority to become the designated router. The higher the value, the higher the priority.

Values 1 — 4294967295

Syntax

priority bootstrap-priority
no priority

Context config>router>pim>rp>bsr-candidate

Description This command configures the bootstrap priority of the router. The RP is sometimes called the bootstrap router. The priority determines if the router is eligible to be a bootstrap router. In the case of a tie, the router with the highest IP address is elected to be the bootstrap router.

Default 0

Parameters bootstrap-priority — Specifies the priority to become the bootstrap router. The higher the value, the higher the priority. A 0 value the router is not eligible to be the bootstrap router. A value of 1 means router is the least likely to become the designated router.

Values 0 — 255

priority

Syntax priority priority
no priority

Context config>router>pim>rp>rp-candidate
cfg>router>pim>rp>ipv6>rp-candidate

Description This command configures the Candidate-RP priority for becoming a rendezvous point (RP). This value is used to elect RP for a group range.

Default 192

Parameters priority — Specifies the priority to become a rendezvous point (RP). A value of 0 is considered as the highest priority.

Values 0 — 255

sticky-dr

Syntax sticky-dr [priority dr-priority]
no sticky-dr

Context config>router>pim>interface
Description

This command enables sticky-dr operation on this interface. When enabled, the priority in PIM hellos sent on this interface when elected as the designated router (DR) will be modified to the value configured in `dr-priority`. This is done to avoid the delays in forwarding caused by DR recovery, when switching back to the old DR on a LAN when it comes back up.

By enabling `sticky-dr` on this interface, it will continue to act as the DR for the LAN even after the old DR comes back up.

The `no` form of the command disables sticky-dr operation on this interface.

Default disabled

Parameters

- `priority dr-priority` — Sets the DR priority to be sent in PIM Hello messages following the election of that interface as the DR, when sticky-dr operation is enabled.

Values

- 1 — 4294967295

three-way-hello

Syntax

- `three-way-hello [compatibility-mode]`
- `no three-way-hello`

Context

- `config>router>pim>interface`

Description

This command configures the compatibility mode to enable three-way hello. By default value is disabled on all interface which specifies that the standard two-way hello is supported. When enabled, the three way hello is supported.

Default no three-way-hello

tracking-support

Syntax

- `[no] tracking-support`

Context

- `config>router>pim>interface`

Description

This command sets the the T bit in the LAN Prune Delay option of the Hello Message. This indicates the router's capability to enable join message suppression. This capability allows for upstream routers to explicitly track join membership.

Default no tracking-support

rp

Syntax

- `rp`

Context

- `config>router>pim`
Router PIM Commands

Description This command enables the context to configure rendezvous point (RP) parameters. The address of the root of the group’s shared multicast distribution tree is known as its RP. Packets received from a source upstream and join messages from downstream routers rendezvous at this router.
If this command is not enabled, then the router can never become the RP.

ipv6

Syntax ipv6
Context config>router>pim>rp
Description This command enables the context to configure IPv6 parameters.

anycast

Syntax [no] anycast rp-ip-address
Context config>router>pim>rp
cfg>router>pim>rp>ipv6
Description This command configures a PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.
The no form of the command removes the anycast instance from the configuration.
Default none
Parameters rp-ip-address — Configure the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address will be replaced with the new address. If no ip-address is entered then the command is simply used to enter the anycast CLI level.
Values Any valid loopback address configured on the node.

auto-rp-discovery

Syntax [no] auto-rp-discovery
Context config>router>pim>rp
Description This command enables Auto-RP protocol in discovery mode. In discovery mode, RP-mapping and RP-candidate messages are received and forwarded to downstream nodes. RP-mapping messages are received locally to learn about availability of RP nodes present in the network.
The no form of the command disables auto RP.
Default no auto-rp-discovery
rp-set-peer

Syntax  [no] rp-set-peer ip-address

Context  config>router>pim>rp>anycast
         config>router>pim>rp>ipv6>anycast

Description  This command configures a peer in the anycast rp-set. The address identifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this rp-set.

Although there is no set maximum number of addresses that can be configured in an rp-set, up to 15 IP addresses is recommended.

The no form of the command removes an entry from the list.

Default  None

Parameters  ip-address — Specifies a peer in the anycast rp-set.

Values  Any valid ip-address within the scope outlined above.

bsr-candidate

Syntax  bsr-candidate

Context  config>router>pim>rp
         config>router>pim>rp>ipv6

Description  This command enables the context to configure Candidate Bootstrap (BSR) parameters.

rp-candidate

Syntax  rp-candidate

Context  config>router>pim>rp
         config>router>pim>rp>ipv6

Description  This command enables the context to configure the Candidate RP parameters.

Routers use a set of available rendezvous points distributed in Bootstrap messages to get the proper group-to-RP mapping. A set of routers within a domain are also configured as candidate RPs (C-RPs); typically these will be the same routers that are configured as candidate BSRs.

Every multicast group has a shared tree through which receivers learn about new multicast sources and new receivers learn about all multicast sources. The rendezvous point (RP) is the root of this shared tree.

Default  shutdown
static

Syntax static

Context config>router>pim>rp
config>router>pim>rp>ipv6

Description This command enables the context to configure static Rendezvous Point (RP) addresses for a multicast group range.

Entries can be created or destroyed. If no IP addresses are configured in the config>router>pim>rp>static>address context, then the multicast group to RP mapping is derived from the RP-set messages received from the Bootstrap Router.

address

Syntax address ip-address

Context config>router>pim>rp>bsr-candidate
config>router>pim>rp>ipv6>bsr-cand

Description This command is used to configure the candidate BSR IP address. This address is for Bootstrap router election.

Default none

Parameters ip-address — The ip-address portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 – 223.255.255.255

address

Syntax [no] address ip-address

Context config>router>pim>rp>rp-candidate
config>router>pim>rp>ipv6>bsr-cand

Description This command configures the local RP address. This address is sent in the RP candidate advertisements to the bootstrap router.

Default none

Parameters ip-address — The ip-address.

Values 1.0.0.0 – 223.255.255.255
address

Syntax  address ip-address
        no address

Context  config>router>pim>rp>static
         config>router>pim>rp>ipv6>static

Description  This command indicates the Rendezvous Point (RP) address that should be used by the router for the range of multicast groups configured by the range command.

Default  none

Parameters  ip-address — The static IP address of the RP. The ip-addr portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values  1.0.0.0 – 223.255.255.255

embedded-rp

Syntax  [no] embedded-rp

Context  config>router>pim>rp>ipv6

Description  This command enables the context to configure embedded RP parameters.

Embedded RP is required to support IPv6 inter-domain multicast because there is no MSDP equivalent in IPv6.

The detailed protocol specification is defined in RFC 3956, Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address. This RFC describes a multicast address allocation policy in which the address of the RP is encoded in the IPv6 multicast group address, and specifies a PIM-SM group-to-RP mapping to use the encoding, leveraging, and extending unicast-prefix-based addressing. This mechanism not only provides a simple solution for IPv6 inter-domain ASM but can be used as a simple solution for IPv6 intra-domain ASM with scoped multicast addresses as well. It can also be used as an automatic RP discovery mechanism in those deployment scenarios that would have previously used the Bootstrap Router protocol (BSR).

The no form of the command disables embedded RP.

group-range

Syntax  [no] group-range ipv6-address/prefix-length

Context  config>router>pim>ipv6>rp>embedded-rp

Description  This command defines which multicast groups can embed RP address information besides FF70::/12.

Embedded RP information is only used when the multicast group is in FF70::/12 or the configured group range.
Parameters *ipv6-address/prefix-length* — Specifies the group range for embedded RP.

**Values**
- **ipv6-address**: x:x:x:x:x:x:x:x (eight 16-bit pieces)  
  x:x:x:x:x:d.d.d  
  x: [0..FFFF]H  
  d: [0..255]D  
- **prefix-length**: 16 — 128

**group-range**

**Syntax**
```
[no] group-range {grp-ip-address/mask | grp-ip-address netmask}
```

**Context**
- config>router>pim>rp>rp-candidate  
- config>router>pim>rp>static>rp>ipv6>rp-candidate

**Description**
This command configures the address ranges of the multicast groups for which this router can be an RP.

**Default**
none

**Parameters**
- **grp-ip-address** — The multicast group IP address expressed in dotted decimal notation.
  **Values**
  - IPv4: a.b.c.d  
  - IPv4-prefix-length: 0 — 32  
  - IPv6-prefix: x:x:x:x:x:x:x:x (eight 16-bit pieces)  
  - IPv6-prefix-length: 16 — 128

- **mask** — The mask associated with the IP prefix expressed as a mask length or in dotted decimal notation; for example /16 for a sixteen-bit mask. The mask can also be entered in dotted decimal notation (255.255.0.0).
  **Values**
  - IPv4-mask: 4 — 32

- **netmask** — The subnet mask in dotted decimal notation.
  **Values**
  - IPv4-netmask: 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

**group-range**

**Syntax**
```
[no] group-range {ip-prefix/mask | ip-prefix netmask}
```

**Context**
config>router>pim>ssm-groups

**Description**
This command configures the address ranges of the multicast groups for this router.

**Default**
none

**Parameters**
- **ip-prefix/mask** — The IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.
  **Values**
  - IPv4-prefix: a.b.c.d  
  - IPv4-prefix-length: 0 — 32  
  - IPv6-prefix: x:x:x:x:x:x:x:x (eight 16-bit pieces)  
  - IPv6-prefix-length: 16 — 128  
  - IPv6-prefix-length: 16 — 128

Page 126 7450 ESS OS Routing Protocols Guide
**Values**

Values 0 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)

`netmask` — The subnet mask in dotted decimal notation.

**Values**

0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

---

**Holdtime**

**Syntax**

```plaintext
holdtime holdtime
no holdtime
```

**Context**

```plaintext
config>router>pim>rp>rp-candidate
config>router>pim>rp>ipv6>rp-candidate
```

**Description**

This command configures the length of time, in seconds, that neighbors should consider the sending router to be operationally up. A local RP cannot be configured on a logical router.

**Parameters**

`holdtime` — Specifies the hold time, in seconds.

**Values**

5 — 255

---

**Group-prefix**

**Syntax**

```plaintext
[group-prefix] {grp-ip-address/mask | grp-ip-address netmask}
```

**Context**

```plaintext
config>router>pim>rp>static>address
config>router>pim>rp>ipv6>static>address
```

**Description**

This command specifies the range of multicast group addresses which should be used by the router as the Rendezvous Point (RP). The `config>router>pim>rp>static>address a.b.c.d` implicitly defaults to deny all for all multicast groups (224.0.0.0/4). A group-prefix must be specified for that static address. This command does not apply to the whole group range.

The `no` form of the command removes the group-prefix from the configuration.

**Default**

none

**Parameters**

`grp-ip-address` — The multicast group IP address expressed in dotted decimal notation.

**Values**

224.0.0.0 — 239.255.255.255

`mask` — The mask associated with the IP prefix expressed as a mask length or in dotted decimal notation; for example `/16` for a sixteen-bit mask. The mask can also be entered in dotted decimal notation (255.255.0.0).

**Values**

4 — 32

`netmask` — The subnet mask in dotted decimal notation.

**Values**

0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)
override

Syntax  [no] override

Context  config>router>pim>rp>static>address
        config>router>pim>rp>ipv6>static>address

Description  This command changes the precedence of static RP over dynamically learned Rendezvous Point (RP).
              When enabled, the static group-to-RP mappings take precedence over the dynamically learned mappings.

Default  no override

non-dr-attract-traffic

Syntax  [no] non-dr-attract-traffic

Context  config>router>pim

Description  This command specifies whether the router should ignore the designated router state and attract traffic even when it is not the designater router.

An operator can configure an interface (router or IES or VPRN interfaces) to IGMP and PIM. The interface state will be synchronized to the backup node if it is associated with the redundant peer port. The interface can be configured to use PIM which will cause multicast streams to be sent to the elected DR only. The DR will also be the router sending traffic to the DSLAM. Since it may be required to attract traffic to both routers a flag non-dr-attract-traffic can be used in the PIM context to have the router ignore the DR state and attract traffic when not DR. Note that while using this flag the router may not send the stream down to the DSLAM while not DR.

When enabled, the designated router state is ignored. When disabled, no non-dr-attract-traffic, the designated router value is honored.

Default  no non-dr-attract-traffic

rpf6-table

Syntax  rpf6-table {rtable6-m | rtable6-u | both}
        no rpf6-table

Context  config>router>pim
        config>router>msdp

Description  This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a particular multicast route.

By default, only the unicast route table is looked up to calculate RPF interface towards the source/rendezvous point. However the operator can specify the following:

a) Use unicast route table only

b) Use multicast route table only or
c) Use both the route tables.

**Parameters**

- **rtable6-m** — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv6 RPF checks. This route table will contain routes submitted by static routes, ISIS and OSPF.
- **rtable6-u** — Specifies only that the unicast route table will be used by the multicast protocol (PIM) for IPv6 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.
- **both** — Will always lookup first in the multicast route table and if there is a route, it will use it. If PIM does not find a route in the first lookup, it will try to find it in the unicast route table. Rtable6-m is checked before rtable6-u.

**Default**

- rtable-u

**sa-timeout**

**Syntax**

```plaintext
sa-timeout seconds
no sa-timeout
```

**Context**

config>router>msdp

**Description**

This command configures the value for the SA entries in the cache. If these entries are not refreshed within the timeout value then they are removed from the cache. Normally the entries are refreshed at least once a minute. But under high load with many of MSDP peers the refresh cycle could be incomplete. A higher timeout value (more then 90) could be useful to prevent unstabilities in the MSDP cache.

**Default**

90

**Parameters**

- **seconds** — Specifies the time, in seconds, to wait for a response from the peer before declaring the peer unavailable.

**Values**

- 90 — 600

**spt-switchover-threshold**

**Syntax**

```plaintext
spt-switchover-threshold {grp-ip-address/mask | grp-ip-address netmask} spt-thres
no spt-switchover-threshold {grp-ip-address/mask | grp-ip-address netmask}
```

**Context**

config>router>pim

**Description**

This command configures shortest path (SPT) tree switchover thresholds for group prefixes.

PIM-SM routers with directly connected routers receive multicast traffic initially on a shared tree rooted at the Rendezvous Point (RP). Once the traffic arrives on the shared tree and the source of the traffic is known, a switchover to the SPT tree rooted at the source is attempted.

For a group that falls in the range of a prefix configured in the table, the corresponding threshold value determines when the router should switch over from the shared tree to the source specific tree. The switchover is attempted only if the traffic rate on the shared tree for the group exceeds the configured threshold.
In the absence of any matching prefix in the table, the default behavior is to switchover when the first packet is seen. In the presence of multiple prefixes matching a given group, the most specific entry is used.

**Parameters**

- **grp-ip-address** — The multicast group IP address expressed in dotted decimal notation.
  - **Values** 224.0.0.0 — 239.255.255.255

- **spt-threshold** — Specifies the configured threshold in kilobits per second (kbps) for a group prefix. A switchover is attempted only if the traffic rate on the shared tree for the group exceeds this configured threshold.
  - **Values** 1 — 4294967294 | infinity

- **mask** — The mask associated with the IP prefix expressed as a mask length or in dotted decimal notation; for example /16 for a sixteen-bit mask. The mask can also be entered in dotted decimal notation (255.255.0.0).
  - **Values** 4 — 32

- **infinity** — When the `infinity` keyword is specified, no switchover will occur at any time, regardless of the traffic level is detected. The threshold, in kilobits per second (KBPS), value is 4294967295.

### ssm-groups

**Syntax**

```
[no] ssm-groups
```

**Context** `config>router>pim`

**Description** This command enables the context to enable an ssm-group configuration instance.

### bootstrap-export

**Syntax**

```
bootstrap-export policy-name [..policy-name]
```

**Context** `config>router>pim>rp`

**Description** Use this command to apply export policies to control the flow of bootstrap messages from the RP, and apply them to the PIM configuration. Up to 5 policy names can be specified.

- **Default** no bootstrap-export

**Parameters**

- **policy-name** — Specify the export policy name up to 32 characters in length.
**Description**  
Use this command to apply import policies to control the flow of bootstrap messages to the RP, and apply them to the PIM configuration. Up to 5 policy names can be specified.

**Default**  
nno bootstrap-import

**Parameters**  
*policy-name* — Specify the import policy name up to 32 characters in length.

### hash-mask-len

**Syntax**  
hash-mask-len  
no hash-mask-len

**Context**  
config>router>pim>rp>bsr-candidate  
config>router>pim>rp>ipv6>bsr-candidate

**Description**  
This command is used to configure the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

**Parameters**  
*hash-mask-length* — The hash mask length.

**Values**  
0 — 32
Router Multicast Source Discovery Protocol (MSDP) Commands

msdp

Syntax [no] msdp
Context config>router
Description This command enables a Multicast Source Discovery Protocol (MSDP) instance. When an MSDP instance is created, the protocol is enabled. To start or suspend execution of the MSDP protocol without affecting the configuration, use the [no] shutdown command.

The no form of the command deletes the MSDP protocol instance removing all associated configuration parameters.

Default no msdp

Interactions: In order for the MSDP protocol to function at least one peer must be configured.
When MSDP is configured and started an appropriate event message should be generated.
When the no form of the command is executed all sessions must be terminated and an appropriate event message should be generated.
When all peering sessions are terminated an event message per peer is not required.

active-source-limit

Syntax active-source-limit number
no active-source-limit
Context config>router>msdp
cfg>router>msdp>group
cfg>router>msdp>group>peer
Description This option controls the maximum number of active source messages that will be accepted by Multicast Source Discovery Protocol (MSDP). This effectively controls the number of active sources that can be stored on the system.

The no form of this command reverts the number of source message limit to default operation

Default No limit is placed on the number of source active records

Parameters number — This parameter defines how many active sources can be maintained by MSDP.

Values 0 — 1000000
receive-msdp-msg-rate

Syntax  
```plaintext
receive-msg-rate number interval seconds [threshold number]
no receive-msg-rate
```

Context  
- `config>router>msdp`
- `config>router>msdp>peer`
- `config>router>msdp>group`
- `config>router>msdp>source`

Description  
This command limits the number of Multicast Source Discovery Protocol (MSDP) messages that are read from the TCP session. It is possible that an MSDP/RP router may receive a large number of MSDP protocol message packets in a particular source active message.

The `no` form of this command reverts this active-source limit to default operation.

Default  
No limit is placed on the number of MSDP and source active limit messages will be accepted.

Parameters  
- `number` — Defines the number of MSDP messages (including source active messages) that are read from the TCP session per the number of seconds.
  - Values: 10 — 10000
  - Default: 0

- `interval` — This defines the time that together with the `number` parameter defines the number of MSDP messages (including source active messages) that are read from the TCP session within the configured number of seconds.
  - Values: 1 — 600
  - Default: 0

- `threshold` — This number reflects the number of MSDP messages can be processed before the MSDP message rate limiting function described above is activated; this is of use in particular during at system startup and initialization.
  - Values: 1 — 1000000
  - Default: 0

Interactions:  
Once the number of MSDP packets (including source active messages) defined in the threshold have been processed the rate of all other MSDP packets is rate limited by no longer accepting messages from the TCP session until the time (seconds) has elapsed.

authentication-key

Syntax  
```plaintext
authentication-key [authentication-key|hash-key] [hash|hash2]
no authentication-key
```

Context  
- `config>router>msdp>peer`
- `config>router>msdp>group>peer`
Description
This command configures a Message Digest 5 (MD5) authentication key to be used with a specific Multicast Source Discovery Protocol (MSDP) peering session. The authentication key must be configured per peer as such no global or group configuration is possible.

Default
Authentication-key. All MSDP messages are accepted and the MD5 signature option authentication key is disabled.

Parameters
- **authentication-key** — The authentication key. Allowed values are any string up to 16 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
- **hash-key** — The hash key. The key can be any combination of ASCII characters up to 33 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).
  
  This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

- **hash** — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

- **hash2** — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

---

data-encapsulation

**Syntax**
[no] data-encapsulation

**Context**
config>router>msdp

**Description**
This command configures a rendezvous point (RP) using Multicast Source Discovery Protocol (MSDP) to encapsulate multicast data received in MSDP register messages inside forwarded MSDP source-active messages.

**Default**
data-encapsulation

---

default-peer

**Syntax**
default-peer

**Context**
config>router>msdp>peer
config>router>msdp>group>peer

**Description**
Using the default peer mechanism a peer can be selected as the default Multicast Source Discovery Protocol (MSDP) peer, as a result all source-active messages from the peer will be accepted without the usual peer-reverse-path-forwarding (RPF) check.
The MSDP peer-RPF check is different from the normal multicast RPF checks. The peer-RPF check is used to stop source-active messages from looping. A router validates source-active messages originated from other routers in a deterministic fashion.

A set of rules is applied in order to validate received source-active messages, and the first rule that applies determines the peer-RPF neighbor. All source-active messages from other routers are rejected. The rules applied to source-active messages originating at Router S received at Router R from Router N are as follows:

- If Router N and router S are one and the same, then the message is originated by a direct peer-RPF neighbor and will be accepted.
- If Router N is a configured peer, or a member of the Router R mesh group then its source-active messages are accepted.
- If Router N is the Border Gateway Protocol (BGP) next hop of the active multicast RPF route toward Router S then Router N is the peer-RPF neighbor and its source-active messages are accepted.
- If Router N is an external BGP peer of Router R and the last autonomous system (AS) number in the BGP AS-path to Router S is the same as Router N’s AS number, then Router N is the peer-RPF neighbor, and its source-active messages are accepted.
- If Router N uses the same next hop as the next hop to Router S, then Router N is the peer-RPF neighbor, and its source-active messages are accepted.
- If Router N fits none of the above rules, then Router N is not a peer-RPF neighbor, and its source-active messages are rejected.

**Default**
No default peer is established and all active source messages must be RPF checked.

**export**

**Syntax**
export policy-name [policy-name...(up to 5 max)]
no export

**Context**
config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>msdp>group>peer

**Description**
This command specifies the policies to export source active state from the source active list into Multicast Source Discovery Protocol (MSDP).

**Default**
No export policies are applied and all SA entries are announced.

**Interactions:**
If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

If you configure an export policy at the global level, each individual peer inherits the global policy. If you configure an export policy at the group level, each individual peer in a group inherits the group’s policy. If you configure an export policy at the peer level then policy only applies to the peer where it is configured.

The no form of the command removes all policies from the configuration.
group

Syntax  [no] group  group-name

Context  config>router>msdp

Description  This command enables access to the context to create or modify a Multicast Source Discovery Protocol (MSDP) group. To configure multiple MSDP groups, include multiple group statements.

By default, the group’s options are inherited from the global MSDP options. To override these global options, group-specific options within the group statement can be configured.

In order for a group to be of use at least one peer must be configured.

Default  no group

Parameters  group-name — Species a unique name for the MSDP group.

Interactions:  If the group name provided is already configured then this command only provides the context to configure the options pertaining to this group.

If the group name provided is not already configured, then the group name must be created and the context to configure the parameters pertaining to the group should be provided. In this case the $ prompt to indicate that a new entity (group) is being created should be used.

import

Syntax  import  policy-name [ policy-name...(up to 5 max)]

no import

Context  config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>msdp>group>peer

Description  This command specifies the policies to import source active state from Multicast Source Discovery Protocol (MSDP) into source active list.

Default  No import policies are applied and all source active messages are allowed.

Interactions:  If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The no form of the command removes all policies from the configuration.

If you configure an import policy at the global level, each individual peer inherits the global policy.

If you configure an import policy at the group level, each individual peer in a group inherits the group’s policy.

If you configure an import policy at the peer level then policy only applies to the peer where it is configured.
local-address

**Syntax**

```
local-address address
no local-address
```

**Context**

```
config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>msdp>group>peer
```

**Description**

This command configures the local end of a Multicast Source Discovery Protocol (MSDP) session. In order for MSDP to function at least one peer must be configured. When configuring a peer, you must include this local-address command to configure the local end of the MSDP session. This address must be present on the node and is used to validate incoming connections to the peer and to establish connections to the remote peer.

The no local address format of this command removes the local-address from the configuration.

**Default**

No local address is configured.

**Parameters**

- `address` — Specifies an existing address on the node.

**Interactions:**

If the user enters this command then the address provided is validated and will be used as the local address for MSDP peers from that point. If a subsequent local-address command is entered it will replace the existing configuration and existing session(s) will be terminated.

Similarly when the no form of this command is entered the existing local-address will be removed from the configuration and the existing session(s) will be terminated.

Whenever a session is terminated all information pertaining to and learned from that peer and will be removed.

Whenever a new peering session is created or a peering session is lost an event message should be generated.

mode

**Syntax**

```
mode {mesh-group | standard}
```

**Context**

```
config>router>msdp>group
```

**Description**

This command configures groups of peers in a full mesh topology to limit excessive flooding of source-active messages to neighboring peers.

Multicast Source Discovery Protocol (MSDP) peers can be configured grouped in a full-mesh topology that prevents excessive flooding of source-active messages to neighboring peers.

**Default**

standard (non-meshed)

**Parameters**

- `mesh-group` — Specifies that source-active message received from a mesh group member are always accepted but are not flooded to other members of the same mesh group. These source-active messages are only flooded to non-mesh group peers or members of other mesh groups.

- `standard` — Specifies a non-meshed mode.
Interactions: In a meshed configuration all members of the group must have a peer connection with every other mesh group member. If this rule is not adhered to then unpredictable results may occur.

peer

Syntax \[[\text{no}]\text{ peer peer-address}\]

Context config>router>msdp
config>router>msdp>group

Description This command configures peer parameters. Multicast Source Discovery Protocol (MSDP) must have at least one peer configured. A peer is defined by configuring a local-address that can be used by this node to set up a peering session and the address of a remote MSDP router. It is the address of this remote peer that is configured in this command and it identifies the remote MSDP router address.

After peer relationships are established, the MSDP peers exchange messages to advertise active multicast sources. It may be required to have multiple peering sessions in which case multiple peer statements should be included in the configurations.

By default the options applied to a peer are inherited from the global or group-level. To override these inherited options, include peer-specific options within the peer statement.

At least one peer must be configured for MSDP to function.

Default none

Parameters peer-address — The address configured in this statement must identify the remote MSDP router that the peering session must be established with.

Interactions: If the peer address provided is already a configured peer then this command only provides the context to configure the parameters pertaining to this peer.

If the peer address provided is not already a configured peer, then the peer instance must be created and the context to configure the parameters pertaining to this peer should be provided. In this case the $ prompt to indicate that a new entity (peer) is being created should be used.

The peer address provided will be validated and assuming it is valid it will be used as the remote address for an MSDP peering session. When the no form of this command is entered the existing peering address will be removed from the configuration and the existing session will be terminated. Whenever a session is terminated all source active information pertaining to and learned from that peer and will be removed. Whenever a new peering session is created or a peering session is lost an event message should be generated.

source

Syntax \[[\text{no}]\text{ source ip-prefix/mask}\]

Context config>router>msdp

Description This command limits the number of active source messages the router accepts from sources in the specified address range.
The `no` form of this message removes the source active rate limiter for this source address range.

**Default**
None. The source active `msdp` messages are not rate limited based on the source address range.

**Interactions:**
If the prefix and mask provided is already a configured then this command only provides the context to configure the parameters pertaining to this active source-message filter.

If the prefix and mask provided is not already a configured, then the source node instance must be created and the context to configure the parameters pertaining to this node should be provided. In this case the `#$` prompt to indicate that a new entity (source) is being created should be used.

**Parameters**

- **ip-prefix** — The IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

  **Values**
  
  ip-prefix/mask: ip-prefix a.b.c.d (host bits must be 0)

- **mask** — The subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

  **Values**
  
  0 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)
Multicast CAC Policy Configuration Commands

mcac

Parameters  mcac

Context  config>router
          config>router>pim>if

Description  This command enables the context to configure multicast CAC parameters.

Default  none

policy

Syntax  policy mcac-policy-name
        no policy mcac-policy-name

Context  configure>router>igmp>interface>mcac
         configure>service>vprn>igmp>interface >mcac

Description  This command references the global channel bandwidth definition policy that is used for (H)mcac and HQoS Adjust.

HQoS Adjustment is supported only with redirection enabled. In other words, the policy from the redirected interface is used for HQoS Adjustment.

Hierarchical mcac (Hmcac) is supported only with redirection enabled. In Hmcac, the subscriber is checked first against its bandwidth limits followed by the check on the redirected interface against the bandwidth limits defined under the redirected interface. In the Hmcac case the channel definition policy must be referenced under the redirected interface level.

Parameters  mcac-policy-name — Specifies the name of the global mcac channel definition policy defined under the hierarchy configure>router>mcac>policy.

Default  No policy is referenced.

bundle

Parameters  [no] bundle bundle-name

Context  config>router>mcac>policy

Description  This command creates the context that enables the grouping of MCAC group addresses into bundles.

When a number of multicast groups or BTV channels are grouped into a single bundle, then policing, if a join for a particular MC-group (BTV channel), can depend on whether:
1. There is enough physical bandwidth on the egress interface.
2. The given channel is a mandatory or optional channel.
   - If optional, is there sufficient bandwidth according to the policy settings for the relevant interface.
   - If optional, is there sufficient bandwidth within the bundle.

The `no` form of the command removes the named bundle from the configuration.

**Default** none

**Parameters**
- `bundle-name` — Specifies the multicast bundle name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
- `bw bandwidth` — Defines the bandwidth available to this bundle when unconstrained.

**bandwidth**

**Syntax**
```
bandwidth bandwidth
no bandwidth
```

**Context**
```
config>router>mcac>policy>bundle
```

**Description**
This command configures the MCAC policy bundle maximum bandwidth.

**Parameters**
- `bandwidth` — Specifies the MCAC policy bandwidth.

**channel**

**Parameters**
- `channel start-address end-address bw bandwidth [class {high | low}] [type {mandatory | optional}]`
- `no channel mc-ip-addr mc-ip-addr`

**Context**
```
config>router>mcac>policy>bundle
```

**Description**
This command creates a MC group (range) as a channel within the bundle where it is configured. A join for a particular MC group address (BTV channel) can be accepted depending on:

1) The channel is mandatory:
   - If there is sufficient bandwidth according to the policy settings for the interface. For bundle level, there is no need for a check since all the mandatory channels get bandwidth pre-reserved when created.

2) The channel is optional:
   - If there is sufficient bandwidth according to the policy settings for the interface.
   - If there is sufficient bandwidth inside the bundle.
When the multicast address is already specified in the same bundle then the new entry overwrites the old. If a multicast address is already specified in another bundle then this command will be rejected and an error message is generated.

If the bundle is removed, the policies associated are also removed and every multicast group that was previously policed (because it was in the bundle that contained the policy) becomes free of constraints.

When a new bundle policy is added to a MCAC policy then policing of the these new addresses must be in a gradual fashion. No active multicast groups can be removed. When a leave message is received for an optional channel then the multicast stream should be pruned and subsequent new joins can be denied in accordance to the policy.

It is possible that momentarily there may be insufficient bandwidth, even for mandatory channels, in this bundle.

**Default**

none

**Parameters**

- `start-address end-address` — Specifies the beginning and ending multicast IP addresses that identifies a multicast stream (BTV channel).

  In a source-specific multicast (SSM) application, a source address preceded by a multicast address is used to identify a specific stream. If a source address is specified then the multicast address must be within the configured SSM address range.

- `bw bandwidth` — Specifies the bandwidth required by this channel in kbps.

  If this bandwidth is configured for a mandatory channel then this bandwidth is reserved by subtracting the amount from the total available bandwidth for all potential egress interfaces and the bundle.

  If this bandwidth is configured as an optional channel then this bandwidth must be available for both the bundle and the egress interface requesting the channel to be added. Once the channel has been added the available bandwidth for the bundle and the interface must be reduced by the configured bandwidth of channel.

  **Values**

  10 — 20000 kbps

- `class {high | low}` — Provides deeper classification of channels used in the algorithm when LAG ports change state.

  **Default**

  low

- `type {mandatory | optional}` — Specifies the channel to be either mandatory or optional.

  - `mandatory` — When the `mandatory` keyword is specified, then the bandwidth is reserved by subtracting it from the total available for all the potential egress interfaces and the bundle.

  - `optional` — When the `optional` keyword is specified then the bandwidth must be available on both the bundle and the egress interface that requests the channel to be added. Once the channel has been added the available bandwidth for the bundle and the interface must be reduced by the configured bandwidth of channel.

  **Default**

  optional

- `mc-ip-address mc-ip-address` — Specifies the IP address that identifies a multicast stream (BTV channel). This must be a multicast address in the x.x.x.x format.
In the case of an SSM application, this means a source address preceded by a multicast address to identify a specific stream in the y.y.y/x.x.x format. If a source address is specified, then the multicast address must be within the configured SSM address range.

**mc-constraints**

**Parameters**

- mc-constraints

**Context**

config>router>mcac>policy>bundle
config>router>igmp>group-interface>mcac

**Description**

This command enables the context to configure the level and its associated bandwidth for a bundle or a logical interface.

- Default

  none

**policy**

**Syntax**

- policy policy-name
- no policy

**Context**

configure>router>igmp>interface>mcac
configure>router>igmp>group-interface>mcac
configure>service>vprn>igmp>interface>mcac
configure>service>vprn>igmp>group-interface>mcac

**Description**

This command references the global channel bandwidth definition policy that is used for (H)mcac and HQoS Adjust.

Within the scope of HQoS Adjustment, the channel definition policy under the group-interface is used if redirection is disabled. In such case HQoS Adjustment can be applied to IPoE subscribers in per-sap replication mode.

In case that redirection is enabled, the channel bandwidth definition policy applied under the Layer 3 redirected interface is in effect.

Hierarchical mcac (Hmcac) is supported on two levels simultaneously:

subscriber level and redirected interface in case that redirection is enabled

subscriber level and group-interface level in case that redirection is disabled.

In Hmcac, the subscriber is first checked against its bandwidth limits followed by the check on the redirected interface (or group-interface) against the bandwidth limits there.

In the case that the redirection is enabled but the policy is referenced ONLY under the group-interface, no admission control will be executed (Hmcac or Mcac).

- Default

  No policy is referenced.

- Parameters

  policy-name — Specifies the name of the global mcac channel definition policy defined under the hierarchy configure>router>mcac>policy.
lag-port-down

Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag-port-down lag-id number-down number-lag-port-down level level-id</td>
<td>Configures the bandwidth available both at the interface and bundle level when a specific number of ports in a LAG group fail.</td>
</tr>
<tr>
<td>no lag-port-down lag-id number-down number-lag-port-down</td>
<td></td>
</tr>
</tbody>
</table>

Context

config>router>mcac>policy>bundle>mc-constraints

Default

none

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lag-id —</td>
<td>When the number of ports available in the LAG link is reduced by the number of ports configured in this context then the level-id specified here must be applied.</td>
</tr>
<tr>
<td>number-down number-lag-port-down —</td>
<td>If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.</td>
</tr>
<tr>
<td>level level-id —</td>
<td>Specifies the amount of bandwidth available within a given bundle for MC traffic for a specified level.</td>
</tr>
</tbody>
</table>

number-down

Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number-down number-lag-port-down level level-id</td>
<td>Configures the number of ports down along with level for multicast cac policy on this interface.</td>
</tr>
<tr>
<td>no number-down number-lag-port-down</td>
<td></td>
</tr>
</tbody>
</table>

Context

config>router>pim>if>mcac>mc-constraints

Default

none

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number-down number-lag-port-down —</td>
<td>If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.</td>
</tr>
<tr>
<td>level level-id —</td>
<td>Specifies the amount of bandwidth available within a given bundle for MC traffic for a specified level.</td>
</tr>
</tbody>
</table>

level

Parameters

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level level bw bandwidth</td>
<td></td>
</tr>
<tr>
<td>no level level</td>
<td></td>
</tr>
</tbody>
</table>

Context

config>router>mcac>policy>bundle>mc-constraints
Description
This command configures the amount of bandwidth available within a given bundle for MC traffic for a specified level. The amount of allowable BW for the specified level is expressed in kbps and this can be defined for up to eight different levels.

The no form of the command removes the level from the configuration.

Default
none (If no bandwidth is defined for a given level then no limit is applied.)

Parameters
level — Specifies the bandwidth for a given level. Level 1 has the highest priority. Level 8 has the lowest priority.
Values 1 — 8

bw bandwidth — Specifies the bandwidth, in kbps, for the level.
Values 1 — 2147483647 kbps
Default 1

number-down

Syntax number-down number-lag-port-down level level-id
no number-down number-lag-port-down

Context config>router>igmp>mcac>mc-constraints

Description This command configures the number of ports down along with level for the MCAC policy.

Parameters number-lag-port-down — Specifies the number of ports down along with level for the MCAC policy.
Values 1 — 8

level level-id — Specifies the bandwidth for a given level. Level 1 has the highest priority. Level 8 has the lowest priority.
Values 1 — 8

unconstrained-bw

Syntax unconstrained-bw bandwidth mandatory-bw mandatory-bw
no unconstrained-bw

Context configure>router>igmp>interface>mcac
configure>router>igmp>group-interface>mcac
configure>service>vprn>igmp>interface >mcac
configure>service>vprn>igmp>group-interface >mcac
configure>subscr-mgmt>sub-mcac-policy

Description This command enables Mcac (or Hmcac) function on the corresponding level (subscriber, group-interface or redirected interface). When Mcac (or Hmcac) is enabled and a channel definition policy is referenced, admission control is performed. The allocated bandwidth for optional channels should not exceed the
unconstrained-bw minus the mandatory-bw. The mandatory channels have to stay below the specified value for the mandatory-bw.

In Hmcac, the subscriber is checked first against its bandwidth limits followed by the check on the redirected interface or the group-interface against the bandwidth limits defined there.

In case that redirection is enabled and Hmcac enabled, the channel definition policy must be referenced under the redirected interface level. If it is referenced under the group-interface level, it will be ignored.

Subscriber Mcac (only subscriber is checked for available resources) is supported only with direct subscriber replication (no redirection). In this case the channel definition policy must be referenced under the group-interface.

In the case that the redirection is enabled but the policy is referenced ONLY under the group-interface, no admission control will be executed (Hmcac or Mcac).

**Default**

- **none**

**Parameters**

- **bandwidth** — Specifies the unconstrained bandwidth in kbps for the MCAC policy.
  - **Values**
    - 0 — 2147483647

- **mandatory-bw**
  - **Values**
    - 0 — 2147483647

### default-action

**Parameters**

- **default-action** {accept | discard}

**Context**

- config>router>mcac>policy

**Description**

This command specifies the action to be applied to multicast streams (channels) when the streams do not match any of the multicast addresses defined in the MCAC policy.

When multiple default-action commands are entered, the last command will overwrite the previous command.

- **Default**
  - discard (all multicast stream not defined in a MCAC policy will be discarded)

**Parameters**

- **accept** — Specifies multicast streams (channels) not defined in the MCAC policy will be accepted.
- **discard** — Specifies multicast streams (channels) not defined in the MCAC policy will be dropped.

### shutdown

**Parameters**

- **[no] shutdown**

**Context**

- config>router>mcac>policy>bundle

**Description**

This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.
When an entity is shutdown, the operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shutdown before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system generated configuration files.

The no form of the command puts an entity into the administratively enabled state.

When a shutdown is performed then all constraints placed on either a bundle or an interface are removed and multicast can potentially take up the full bandwidth of the interface. Furthermore, when a no shutdown command is executed then policing of the policy must be in a gradual fashion. No active multicast groups may be removed. When a leave message is received for an optional channel then the multicast stream should be pruned and subsequent new joins can be denied in accordance with the policy. This may mean that for a period of time insufficient bandwidth is available even for mandatory channels.
MLD Commands

mld

Syntax  
[no] mld

Context  
config>router

Description  
This command enables the context to configure Multicast Listener Discovery (MLD) parameters.

The no form of the command disables MLD.

Default  
no mld

interface

Syntax  
[no] interface ip-int-name

Context  
config>router>mld

Description  
This command enables the context to configure an Multicast Listener Discovery (MLD) interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled.

The no form of the command deletes the MLD interface. The shutdown command in the config>router>mld>interface context can be used to disable an interface without removing the configuration for the interface.

Default  
no interface — No interfaces are defined.

Parameters  
ip-int-name — The IP interface name. Interface names must be unique within the group of defined IP interfaces for config router interface and config service ies interface commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

disable-router-alert-check

Syntax  
[no] disable-router-alert-check

Context  
config>router>mld>if

Description  
This command enables router alert checking for MLD messages received on this interface.
The no form of the command disables the router alert checking.

Default none

import

Syntax import policy-name
no import

Context config>router>mld>if

Description This command specifies the import route policy to be used for determining which membership reports are accepted by the router. Route policies are configured in the config>router>policy-options context.

When an import policy is not specified, all the MLD reports are accepted.

The no form of the command removes the policy association from the MLD instance.

Default no import — No import policy specified.

Parameters policy-name — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the config>router>policy-options context.

max-groups

Syntax max-groups value
no max-groups

Context config>router>mld>if

Description This command specifies the maximum number of groups for which MLD can have local receiver information based on received MLD reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

Default 0, no limit to the number of groups.

Parameters value — Specifies the maximum number of groups for this interface.

Values 1 — 16000
query-interval

Syntax

query-interval seconds
no query-interval

Context
config>router>mld
config>router>mld>if

Description
This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default 125

Parameters

seconds — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 — 1024

query-last-member-interval

Syntax

query-last-member-interval seconds

Context
config>router>mld
config>router>mld>if

Description
This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default 1

Parameters

seconds — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 — 1024

query-response-interval

Syntax

query-response-interval seconds

Context
config>router>mld
config>router>mld>if

Description
This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default 10

Parameters

seconds — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values 1 — 1023
static

**Syntax**

static

**Context**

config>router>mld>if

**Description**

This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

**Default**

none

---

**group**

**Syntax**

[no] group ipv6-address

**Context**

config>router>mld>if>static

cfg-router-mld>if>static>group

cfg-router-mld>ssm-translate>grp-range

**Description**

This command enables the context to add a static multicast group either as a (*,G) or one or more (S,G) records. Use MLD static group memberships to test multicast forwarding without a receiver host. When MLD static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static MLD group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static MLD group entries do not generate join messages toward the RP.

The **no** form of the command removes the IPv6 address from the configuration.

**Default**

none

**Parameters**

ipv6-address — Specifies an MLD multicast group address that receives data on an interface. The IP address must be unique for each static group.

---

**source**

**Syntax**

[no] source ipv6-address

**Context**

config>router>mld>if>static>group

config>router>mld>ssm-translate>grp-range

**Description**

This command specifies an IPv6 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the source(s) that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group. The source command, in combination with the group, is used to create a specific (S,G) static group entry.

The **no** form of the command removes the source from the configuration.

**Default**

none

**Parameters**

ip-address — Specifies the IPv6 unicast address.
MLD Commands

starg

Syntax  [no] starg
Context  config>router>mld>if>static>group
Description  This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.
Use the no form of the command to remove the starg entry from the configuration.
Default  none

subnet-check

Syntax  [no] subnet-check
Context  config>router>mld>interface
Description  This command enables subnet checking for MLD messages received on this interface. All MLD packets with a source address that is not in the local subnet are dropped.
Default  enabled

version

Syntax  version version
  no version
Context  config>router>mld>if
Description  This command specifies the MLD version. If routers run different versions, they will negotiate the lowest common version of MLD that is supported by hosts on their subnet and operate in that version. For MLD to function correctly, all routers on a LAN should be configured to run the same version of MLD on that LAN.
Default  1
Parameters  version — Specifies the MLD version number.
  Values  1, 2
robust-count

Syntax

robust-count robust-count
no robust-count

Context config>router>mld

Description This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default 2

Parameters robust-count — Specify the robust count value.

Values 2 — 10

ssm-translate

Syntax ssm-translate

Context config>router>mld

Description This command enables the context to configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the source command with starg command enabled.

grp-range

Syntax [no] grp-range start end

Context config>router>mld>ssm-translate

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters start — An IP address that specifies the start of the group range.
end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the start value.
source

Syntax  [no] source ip-address

Context  config>router>mld>ssm-translate>grp-range

Description  This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by grp-range start and end parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters  ip-address — Specifies the IP address that will be sending data.
Operational Commands

**mrinfo**

**Syntax**

```
mrinfo ip-address [router router-name] [service]
```

**Context**

`<GLOBAL>`

**Description**

This command is used to display relevant multicast information from the target multicast router. Information displayed includes adjacency information, protocol, metrics, thresholds, and flags from the target multicast router. This information can be used by network operators to determine whether bi-directional adjacencies exist.

**Parameters**

- `ip-address` — Specify the IP address of the multicast capable target router should be entered.
- `router router-name` — Specify the router instance that this command applies to.
  - **Default** management Base
- `service` — Specify the service instance that this command applies to.
  - **Values** `1 — 2147483647`

**Mrinfo Output Fields** — The following table describes the output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General flags</td>
<td></td>
</tr>
<tr>
<td>version</td>
<td>Indicates software version on queried router.</td>
</tr>
<tr>
<td>prune</td>
<td>Indicates that router understands pruning.</td>
</tr>
<tr>
<td>genid</td>
<td>Indicates that router sends generation IDs.</td>
</tr>
<tr>
<td>mtrace</td>
<td>Indicates that the router handles mtrace requests.</td>
</tr>
<tr>
<td>Neighbors flags</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Metric</td>
</tr>
<tr>
<td>0</td>
<td>Threshold (multicast time-to-live)</td>
</tr>
<tr>
<td>pim</td>
<td>PIM enabled on interface.</td>
</tr>
<tr>
<td>down</td>
<td>Operational status of interface.</td>
</tr>
<tr>
<td>disabled</td>
<td>Administrative status of interface.</td>
</tr>
<tr>
<td>leaf</td>
<td>No downstream neighbors on interface.</td>
</tr>
<tr>
<td>querier</td>
<td>Interface is IGMP querier.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Neighbor reached via tunnel.</td>
</tr>
</tbody>
</table>
A:dut-f# mrinfo 10.1.1.2

10.1.1.2 [version 3.0,prune,genid,mtrace]:
10.1.1.2 -> 10.1.1.1 [1/0/pim]
16.1.1.1 -> 0.0.0.0 [1/0/pim/down/disabled]
17.1.1.1 -> 0.0.0.0 [1/0/pim/querier/leaf]
200.200.200.3 -> 200.200.200.5 [1/0/tunnel/pim]...

mstat

**Syntax**

```
  mstat source ip-address group grp-ip-address [destination dst-ip-address] [hop hop] [router router-name] [service] [wait-time wait-time]
```

**Context**

<GLOBAL>

**Description**

This command traces a multicast path from a source to a receiver and displays multicast packet rate and loss information. The mstat command adds the capability to show the multicast path in a limited graphic display and provide drops, duplicates, TTLs, and delays at each node. This information is useful to network operators because it identifies nodes with high drop and duplicate counts. Duplicate counts are shown as negative drops.

**Parameters**

- **source ip-address** — Specify the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.
- **group grp-ip-address** — Specify the multicast address that will be used.
- **destination dst-ip-address** — Specify the IP address of the unicast destination. If this parameter is omitted, the IP address of the system where the command is entered is used. The destination parameter can also be used to specify a local interface address as the destination address to send the trace query.
- **hop hop** — Specify the maximum number of hops that will be traced from the receiver back toward the source.
  - **Values** 1 — 255
  - **Default** 32 hops (infinity for the DVMRP routing protocol).
- **router router-name** — Specify the router instance that this command applies to.
- **service** — Specify the service instance that this command applies to.
  - **Values** 1 — 2147483647
- **wait-time wait-time** — Specify the number of seconds to wait for the response.
  - **Values** 1 — 60
  - **Default** 10
**Mstat Output Fields** — The following table describes the output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hop</td>
<td>Number of hops from the source to the listed router.</td>
</tr>
<tr>
<td>router name</td>
<td>Name of the router for this hop or “?” when not reverse DNS translated.</td>
</tr>
<tr>
<td>address</td>
<td>Address of the router for this hop.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol used.</td>
</tr>
<tr>
<td>ttl</td>
<td>Forward TTL threshold. TTL that a packet is required to have before it will be forwarded over the outgoing interface.</td>
</tr>
<tr>
<td>forwarding code</td>
<td>Forwarding information/error code for this hop.</td>
</tr>
</tbody>
</table>

For each interface between 2 nodes a line is printed, following the same layout as other routers with an implementation derived from mrouted. Note the following:

- The forwarding information/error code is only displayed when different from “No Error”.
- “?” means the there is no reverse DNS translation.
- There is no “Overall Mcast Pkt Rate” available in the PE for the VPRN case.
mtrace

**Syntax**

```
mtrace source ip-address group grp-ip-address [destination dst-ip-address] [hop hop] [router router-name|service] [wait-time wait-time]
```

**Context**

```
<GLOBAL>
```

**Description**

This command traces the multicast path from a source to a receiver by passing a trace query hop-by-hop along the reverse path from the receiver to the source. At each hop, information such as the hop address, routing error conditions, and packet statistics are gathered and returned to the requestor. A network administrator can determine where multicast flows stop and verify the flow of the multicast stream.

**Parameters**

- `source ip-address` — Specify the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.
- `group group-ip-address` — Specify the multicast address that will be used.
- `destination dst-ip-address` — Specify the IP address of the unicast destination. If this parameter is omitted, the IP address of the system where the command is entered is used. The destination parameter can also be used to specify a local interface address as the destination address to send the trace query.

**Default**

The default address for the destination address is the incoming IETF format for that (S,G)
**hop hop** — Specify the maximum number of hops that will be traced from the receiver back toward the source.

**Values**

1 — 255

**Default**

32 hops (infinity for the DVMRP routing protocol).

**router router-name** — Specify the router instance that this command applies to.

**service** — Specify the service instance that this command applies to.

**Values**

1 — 2147483647

**wait-time wait-time** — Specify the number of seconds to wait for the response.

**Values**

1 — 60

**Default**

10

**Mtrace Output Fields** — The following table describes the output fields:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hop</td>
<td>Number of hops from the source to the listed router.</td>
</tr>
<tr>
<td>router name</td>
<td>Name of the router for this hop. If a DNS name query is not successful a “?” displays.</td>
</tr>
<tr>
<td>address</td>
<td>Address of the router for this hop.</td>
</tr>
<tr>
<td>protocol</td>
<td>Protocol used.</td>
</tr>
<tr>
<td>ttl</td>
<td>Forward TTL threshold. TTL that a packet is required to have before it will be forwarded over the outgoing interface.</td>
</tr>
<tr>
<td>forwarding code</td>
<td>Forwarding information/error code for this hop.</td>
</tr>
</tbody>
</table>

```
A:Dut-F# mtrace source 10.10.16.9 group 224.5.6.7

Mtrace from 10.10.16.9 via group 224.5.6.7
Querying full reverse path...

  0  ? (10.10.10.6)
-1  ? (10.10.10.5)  PIM  thresh^ 1  No Error
-2  ? (10.10.6.4)  PIM  thresh^ 1  No Error
-3  ? (10.10.4.2)  PIM  thresh^ 1  Reached RP/Core
-4  ? (10.10.1.1)  PIM  thresh^ 1  No Error
-5  ? (10.10.2.3)  PIM  thresh^ 1  No Error
-6  ? (10.10.16.9)

Round trip time 29 ms; total ttl of 5 required.
```
Operational Commands
Show Commands

IGMP Commands

group

Syntax

\[ \text{group [grp-ip-address]} \]
\[ \text{group summary} \]

Context

show>router>igmp

Description

This command displays the multicast group and (S,G) addresses. If no \text{grp-ip-address} parameters are specified then all IGMP group, (*,G) and (S,G) addresses are displayed.

Parameters

\text{grp-ip-address} — Displays specific multicast group addresses.

Output

IGMP Group Output — The following table describes the output fields for IGMP group information.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Groups</td>
<td>Displays the IP multicast sources corresponding to the IP multicast groups which are statically configured.</td>
</tr>
<tr>
<td>Fwd List</td>
<td>Displays the list of interfaces in the forward list.</td>
</tr>
<tr>
<td>Blk List</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

*B:Dut-C# show router igmp group

===============================================================================
IGMP Interface Groups
===============================================================================

===============================================================================
IGMP Host Groups
===============================================================================

(*,225.0.0.1)
| Fwd List : 112.112.1.2 | Up Time : 0d 00:00:21 |

(11.11.0.1,225.0.0.1)
| Fwd List : 112.112.1.1 | Up Time : 0d 00:00:30 |
| Blk List : 112.112.1.2 | Up Time : 0d 00:00:21 |

(11.11.0.2,225.0.0.1)
| Fwd List : 112.112.1.1 | Up Time : 0d 00:00:30 |

(*,225.0.0.2)
| Fwd List : 112.112.1.2 | Up Time : 0d 00:00:21 |

(11.11.0.1.2,225.0.0.2)
| Blk List : 112.112.1.2 | Up Time : 0d 00:00:21 |

(*,G)/(S,G) Entries : 5

===============================================================================

7450 ESS OS Routing Protocols Guide
hosts

Syntax hosts [group grp-address] [detail] [fwd-service service-id] [grp-interface ip-int-name] hosts [host ip-address] [group grp-address] [detail] hosts summary

Context show>router>igmp

Description This command shows IGMP hosts information.

Sample Output

*B:Dut-C# show router igmp hosts

IGMP Hosts

<table>
<thead>
<tr>
<th>Host</th>
<th>Oper State</th>
<th>Oper Version</th>
<th>Fwd Svc</th>
<th>GrpItf</th>
<th>Num Groups</th>
<th>Subscriber</th>
</tr>
</thead>
<tbody>
<tr>
<td>112.112.1.1</td>
<td>Up</td>
<td>3</td>
<td>1</td>
<td>gi_1_1</td>
<td>1</td>
<td>sub_1</td>
</tr>
<tr>
<td>112.112.1.2</td>
<td>Up</td>
<td>3</td>
<td>1</td>
<td>gi_1_1</td>
<td>2</td>
<td>sub_1</td>
</tr>
<tr>
<td>112.112.1.3</td>
<td>Up</td>
<td>3</td>
<td>1</td>
<td>gi_1_2</td>
<td>0</td>
<td>sub_2</td>
</tr>
</tbody>
</table>

Hosts : 3
*B:Dut-C#

*B:Dut-C# show router igmp hosts detail

<table>
<thead>
<tr>
<th>IGMP Host 112.112.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper Status          : Up</td>
</tr>
<tr>
<td>Oper version         : 3</td>
</tr>
<tr>
<td>Num Groups           : 1</td>
</tr>
<tr>
<td>Max Grps Till Now    : 2</td>
</tr>
<tr>
<td>PPPoE SessionId      : 1</td>
</tr>
<tr>
<td>FwdSvcId             : 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IGMP Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address : 225.0.0.1</td>
</tr>
<tr>
<td>Expires : Not running</td>
</tr>
<tr>
<td>V1 Host Timer : Not running</td>
</tr>
<tr>
<td>V2 Host Timer : Not running</td>
</tr>
<tr>
<td>Redir.vRtrId : N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Expires</th>
<th>Type</th>
<th>Fwd/Blk</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.11.0.1</td>
<td>0d 00:03:56</td>
<td>Dynamic</td>
<td>Fwd</td>
</tr>
<tr>
<td>11.11.0.2</td>
<td>0d 00:03:56</td>
<td>Dynamic</td>
<td>Fwd</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IGMP Host 112.112.1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oper Status          : Up</td>
</tr>
<tr>
<td>Oper version         : 3</td>
</tr>
<tr>
<td>Num Groups           : 2</td>
</tr>
<tr>
<td>Max Grps Till Now    : 2</td>
</tr>
<tr>
<td>PPPoE SessionId      : 2</td>
</tr>
<tr>
<td>FwdSvcId             : 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IGMP Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address : 225.0.0.1</td>
</tr>
<tr>
<td>Expires : 0d 00:04:05</td>
</tr>
<tr>
<td>V1 Host Timer : Not running</td>
</tr>
<tr>
<td>V2 Host Timer : Not running</td>
</tr>
<tr>
<td>Redir.vRtrId : N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Expires</th>
<th>Type</th>
<th>Fwd/Blk</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.11.0.1</td>
<td>0d 00:00:00</td>
<td>Dynamic</td>
<td>Blk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IGMP Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address : 225.0.0.2</td>
</tr>
<tr>
<td>Expires : 0d 00:04:04</td>
</tr>
<tr>
<td>V1 Host Timer : Not running</td>
</tr>
<tr>
<td>V2 Host Timer : Not running</td>
</tr>
<tr>
<td>Redir.vRtrId : N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Expires</th>
<th>Type</th>
<th>Fwd/Blk</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.11.0.1</td>
<td>0d 00:00:00</td>
<td>Dynamic</td>
<td>Blk</td>
</tr>
</tbody>
</table>
IGMP Host 112.112.1.3

Oper Status : Up  MacAddress : 00:00:00:00:00:02
Oper version : 3  Subscriber : sub_2
Num Groups : 0  GrpItf : gi_1_2
Max Grps Till Now: 1  IGMP-Policy : pol1
PPPoE SessionId : 1  Next query time: 0d 00:00:48
FwdSvcId : 1

Hosts : 3

*B:Dut-C#

*B:Dut-C# show router igmp statistics host 112.112.1.1

IGMP Host Statistics 112.112.1.1

Message Type  Received  Transmitted
-----------------------------
Queries 0 580
Report V1 0 0
Report V2 0 0
Report V3 5 0
Leaves 0 0

General Host Statistics
-----------------------------
Bad Length : 0
Bad Checksum : 0
Unknown Type : 0
Bad Receive If : 0
Rx Non Local : 0
Rx Wrong Version : 0
Policy Drops : 0
No Router Alert : 0
Rx Bad Encodings : 0
Local Scope Pkts : 0
Resvd Scope Pkts : 0
MCAC Policy Drops : 0

Source Group Statistics
-----------------------------
(S,G) : 0
(*,G) : 0

*B:Dut-C# show subscriber-mgmt igmp-policy
**ssm-translate**

**Syntax**

```
ssm-translate
ssm-translate interface interface-name
```

**Context**

```
show>router>igmp
```

**Description**

This command displays IGMP SSM translate configuration information.

**Output**

**GMP Interface Output** — The following table provides IGMP field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Range</td>
<td>Displays the address ranges of the multicast groups for which this router can be an RP.</td>
</tr>
<tr>
<td>Source</td>
<td>Displays the unicast address that sends data on an interface.</td>
</tr>
<tr>
<td>SSM Translate Entries</td>
<td>Displays the total number of SSM translate entries.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
=================================================================================
IGMP SSM Translate Entries
=================================================================================
Group Range Source    Interface
<234.1.1.1 - 234.1.1.2> 100.1.1.1            -
<232.1.1.1 - 232.1.1.5> 100.1.1.2           ies-abc
=================================================================================
```

**interface**

**Syntax**

```
interface [ip-int-name | ip-address] [group] [grp-address] [detail]
```

**Context**

```
show>router>igmp
```

**Description**

This command displays IGMP interface information.

**Parameters**

- `ip-int-name` — Only displays the information associated with the specified IP interface name.
- `ip-address` — Only displays the information associated with the specified IP address.
- `group grp-address` — Only displays IP multicast group address for which this entry contains information.
- `detail` — Displays detailed IP interface information along with the source group information learned on that interface.
### IGMP Interface Output

The following table provides IGMP field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Specifies the interfaces that participate in the IGMP protocol.</td>
</tr>
<tr>
<td>Adm Admin Status</td>
<td>Displays the administrative state for the IGMP protocol on this interface.</td>
</tr>
<tr>
<td>Oper Oper Status</td>
<td>Displays the current operational state of IGMP protocol on the interface.</td>
</tr>
<tr>
<td>Querier</td>
<td>Displays the address of the IGMP querier on the IP subnet to which the interface is attached.</td>
</tr>
<tr>
<td>Querier Up Time</td>
<td>Displays the time since the querier was last elected as querier.</td>
</tr>
<tr>
<td>Querier Expiry Timer</td>
<td>Displays the time remaining before the querier ages out. If the querier is the local interface address, the value will be zero.</td>
</tr>
<tr>
<td>Cfg/Opr Version</td>
<td>Cfg — The configured version of IGMP running on this interface. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.</td>
</tr>
<tr>
<td>Policy</td>
<td>Specifies the policy that is to be applied on the interface.</td>
</tr>
<tr>
<td>Group Address</td>
<td>Specifies the IP multicast group address for which this entry contains information.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Specifies the time since this source group entry got created.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>Specifies the IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.</td>
</tr>
<tr>
<td>Mode</td>
<td>The mode is based on the type of membership report(s) received on the interface for the group. In the 'include' mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter of the IGMP membership report. In 'exclude' mode, reception of packets sent to the given multicast address is requested from all IP source addresses except those listed in the source-list parameter.</td>
</tr>
</tbody>
</table>
Multicast

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1 Host Timer</td>
<td>The time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. Upon hearing any IGMPv1 Membership Report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv2 Leave messages for this group that it receives on this interface.</td>
</tr>
<tr>
<td>V2 Host Timer</td>
<td>The time remaining until the local router will assume that there are no longer any IGMP version 2 members on the IP subnet attached to this interface. Upon hearing any IGMPv2 Membership Report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv3 Leave messages for this group that it receives on this interface.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates how this group entry was learned. If this group entry was learned by IGMP, it will be set to “dynamic”. For statically configured groups, the value will be set to 'static'.</td>
</tr>
<tr>
<td>Compat Mode</td>
<td>Used in order for routers to be compatible with older version routers. IGMPv3 hosts MUST operate in version 1 and version 2 compatibility modes. IGMPv3 hosts MUST keep state per local interface regarding the compatibility mode of each attached network. A host's compatibility mode is determined from the Host Compatibility Mode variable which can be in one of three states: IGMPv1, IGMPv2 or IGMPv3. This variable is kept per interface and is dependent on the version of General Queries heard on that interface as well as the Older Version Querier Present timers for the interface.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-BA# show router 100 interface

Interface Table (Service: 100)

<table>
<thead>
<tr>
<th>Interface-Name</th>
<th>IP-Address</th>
<th>Adm</th>
<th>Opr(v4/v6)</th>
<th>Mode</th>
<th>Port/SapId</th>
<th>PfxState</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP_to_CE</td>
<td>11.1.1.1/24</td>
<td>Up</td>
<td>Up</td>
<td>VPRN</td>
<td>1/1/7</td>
<td>n/a</td>
</tr>
<tr>
<td>system</td>
<td>10.20.1.2/32</td>
<td>Up</td>
<td>Up</td>
<td>VPRN</td>
<td>loopback</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Interfaces: 2

*A:ALA-BA#

*A:ALA-BA# show router 100 interface IGMP_to_CE

Interface Table (Service: 100)
### IGMP Commands

<table>
<thead>
<tr>
<th>IP-Address</th>
<th>PfxState</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP_to_CE</td>
<td>Up</td>
</tr>
<tr>
<td>11.1.1.1/24</td>
<td>Up</td>
</tr>
</tbody>
</table>

**IGMP Interfaces**

```
*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface
```

**IGMP Interfaces**

```
Interface          Adm  Oper Querier Cfg/Opr Num Policy
Version Groups
---------------------------------------------------
IGMP_to_CE         Up   Up   11.1.1.1        1/1     3     igmppol
```

**IGMP Interface IGMP_to_CE**

```
*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface IGMP_to_CE
```

**IGMP Interface IGMP_to_CE**

```
Interface          Adm  Oper Querier Cfg/Opr Num Policy
Version Groups
---------------------------------------------------
IGMP_to_CE         Up   Up   11.1.1.1        1/1     3     igmppol
```

**IGMP Interface 11.1.1.1**

```
*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface 11.1.1.1
```

**IGMP Interface 11.1.1.1**

```
Interface          Adm  Oper Querier Cfg/Opr Num Policy
Version Groups
---------------------------------------------------
IGMP_to_CE         Up   Up   11.1.1.1        1/1     3     igmppol
```

**IGMP Interface 11.1.1.1**

```
*A:ALA-BA#
```

---

Page 168  7450 ESS OS Routing Protocols Guide
*A:ALA-BA# show router 100 igmp interface IGMP_to_CE group 227.1.1.1

IGMP Interface IGMP_to_CE

<table>
<thead>
<tr>
<th>Interface</th>
<th>Adm</th>
<th>Oper</th>
<th>Querier</th>
<th>Cfg/Opr Num</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP_to_CE</td>
<td>Up</td>
<td>Up</td>
<td>11.1.1.1</td>
<td>1/1</td>
<td>3</td>
</tr>
</tbody>
</table>

IGMP Group

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Up Time</th>
<th>Expires</th>
<th>Last Reporter</th>
<th>Mode</th>
<th>V1 Host Timer</th>
<th>V2 Host Timer</th>
<th>V1 Host Timer</th>
<th>V2 Host Timer</th>
<th>V1 Host Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td>227.1.1.1</td>
<td>0d 00:03:52</td>
<td>never</td>
<td>0.0.0.0</td>
<td>exclude</td>
<td>Not running</td>
<td>Not running</td>
<td>Not running</td>
<td>Not running</td>
<td>Not running</td>
</tr>
</tbody>
</table>

Interfaces : 1

*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface IGMP_to_CE group 227.1.1.1 detail

IGMP Interface IGMP_to_CE

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin Status</th>
<th>Oper Status</th>
<th>Querier</th>
<th>Querier Up Time</th>
<th>Querier Expiry Time</th>
<th>Admin/Oper version</th>
<th>Policy</th>
<th>Subnet Check</th>
<th>MCAC Policy Name</th>
<th>MCAC Max Unconst BW</th>
<th>MCAC Max Mand BW</th>
<th>MCAC In use Mand BW</th>
<th>MCAC Avail Mand BW</th>
<th>MCAC In use Opnl BW</th>
<th>MCAC Avail Opnl BW</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP_to_CE</td>
<td>Up</td>
<td>Up</td>
<td>11.1.1.1</td>
<td>0d 00:04:01</td>
<td>N/A</td>
<td>1/1</td>
<td>igmppol</td>
<td>Disabled</td>
<td></td>
<td>no limit</td>
<td>no limit</td>
<td>0</td>
<td>unlimited</td>
<td>0</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

IGMP Group

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Up Time</th>
<th>Expires</th>
<th>Last Reporter</th>
<th>Mode</th>
<th>V1 Host Timer</th>
<th>V2 Host Timer</th>
<th>V1 Host Timer</th>
<th>V2 Host Timer</th>
<th>V1 Host Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td>227.1.1.1</td>
<td>0d 00:04:02</td>
<td>never</td>
<td>0.0.0.0</td>
<td>exclude</td>
<td>Not running</td>
<td>Not running</td>
<td>Not running</td>
<td>Not running</td>
<td>Not running</td>
</tr>
</tbody>
</table>

Interfaces : 1

*A:ALA-BA#
static

**Syntax**

\[
\text{static [ip-int-name | ip-addr]}
\]

**Context**

show>router>igmp

**Description**

This command displays static IGMP, (*.G) and (S.G) information.

**Parameters**

- **ip-int-name** — Only displays the information associated with the specified IP interface name.
- **ip-addr** — Only displays the information associated with the specified IP address.

**Output**

**Static IGMP Output** — The following table provides static IGMP field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Displays entries which represents a source address from which receivers are interested/not interested in receiving multicast traffic.</td>
</tr>
<tr>
<td>Group</td>
<td>Displays the IP multicast group address for which this entry contains information.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the interface name.</td>
</tr>
</tbody>
</table>

**Sample Output**

*A:ALA-BA# show router 100 igmp static

================================================================================
IGMP Static Group Source
================================================================================
<table>
<thead>
<tr>
<th>Source</th>
<th>Group</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.11.11.11</td>
<td>226.136.22.3</td>
<td>IGMP_to_CE</td>
</tr>
<tr>
<td>*</td>
<td>227.1.1.1</td>
<td>IGMP_to_CE</td>
</tr>
<tr>
<td>22.22.22.22</td>
<td>239.255.255.255</td>
<td>IGMP_to_CE</td>
</tr>
</tbody>
</table>
================================================================================
Static (*.G)/(S,G) Entries : 3
================================================================================
*A:ALA-BA#|

statistics

**Syntax**

\[
\text{statistics [ip-int-name | ip-address]}
\]

**Context**

show>router>igmp

**Description**

This command displays IGMP statistics information.

**Parameters**

- **ip-int-name** — Only displays the information associated with the specified IP interface name.
- **ip-address** — Only displays the information associated with the specified IP address.
Output IGMP Statistics Output — The following table provides statistical IGMP field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP Interface Statistics</td>
<td>The section listing the IGMP statistics for a particular interface.</td>
</tr>
<tr>
<td>Message Type Queries</td>
<td>The number of IGMP general queries transmitted or received on this interface.</td>
</tr>
<tr>
<td>Report</td>
<td>The total number of IGMP V1, V2, or V3 reports transmitted or received on this interface.</td>
</tr>
<tr>
<td>Leaves</td>
<td>The total number of IGMP leaves transmitted on this interface.</td>
</tr>
<tr>
<td>Received</td>
<td>Displays the total number of IGMP packets received on this interface.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Column that displays the total number of IGMP packets transmitted from this interface.</td>
</tr>
<tr>
<td>General Interface Statistics</td>
<td>The section listing the general IGMP statistics.</td>
</tr>
<tr>
<td>Bad Length</td>
<td>Displays the total number of IGMP packets with bad length received on this interface.</td>
</tr>
<tr>
<td>Bad Checksum</td>
<td>Displays the total number of IGMP packets with bad checksum received on this interface.</td>
</tr>
<tr>
<td>Unknown Type</td>
<td>Displays the total number of IGMP packets with unknown type received on this interface.</td>
</tr>
<tr>
<td>Bad Receive If</td>
<td>Displays the total number of IGMP packets incorrectly received on this interface.</td>
</tr>
<tr>
<td>Rx Non Local</td>
<td>Displays the total number of IGMP packets received from a non-local sender.</td>
</tr>
<tr>
<td>Rx Wrong Version</td>
<td>Displays the total number of IGMP packets with wrong versions received on this interface.</td>
</tr>
<tr>
<td>Policy Drops</td>
<td>Displays the total number of times IGMP protocol instance matched the host IP address or group/source addresses specified in the import policy.</td>
</tr>
<tr>
<td>No Router Alert</td>
<td>Displays the total number of IGMPv3 packets received on this interface which did not have the router alert flag set.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-BA# show router 100 igmp statistics

IGMP Interface Statistics

Message Type | Received | Transmitted
--------------|----------|------------
Queries       | 0        | 5          
Report V1     | 0        | 0          
Report V2     | 0        | 0          
Report V3     | 0        | 0          
Leaves        | 0        | 0          

General Interface Statistics

Bad Length    : 0
Bad Checksum  : 0
Unknown Type  : 0
Bad Receive If: 0
Rx Non Local  : 0
Rx Wrong Version : 0
Policy Drops  : 0
No Router Alert : 0
Rx Bad Encodings : 0
Rx Pkt Drops  : 0

Source Group Statistics

(S,G)         : 2
(*,G)         : 1

*A:ALA-BA#

*B:Dut-C# show router igmp statistics host

IGMP Host Statistics

Message Type | Received | Transmitted
--------------|----------|------------
Queries       | 0        | 1739       
Report V1     | 0        | 0          
Report V2     | 0        | 0          
Report V3     | 10       | 0          
Leaves        | 0        | 0          

General Host Statistics

Bad Length    : 0
Bad Checksum  : 0
Unknown Type  : 0
Bad Receive If: 0
Rx Non Local  : 0
Rx Wrong Version : 0
Policy Drops  : 0
No Router Alert : 0
Rx Bad Encodings : 0
Local Scope Pkts : 0
status

Syntax status

Context show>router>igmp

Description This command displays IGMP status information.
If IGMP is not enabled, the following message appears:
A:NYC# show router igmp status
MINOR: CLI IGMP is not configured.
A:NYC#

Output IGMP Status Output — The following table provides IGMP status field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Displays the administrative status of IGMP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Displays the current operating status of this IGMP protocol instance on this router.</td>
</tr>
<tr>
<td>Query Interval</td>
<td>The frequency at which IGMP query packets are transmitted.</td>
</tr>
<tr>
<td>Last Member Query Interval</td>
<td>The maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages.</td>
</tr>
<tr>
<td>Query Response Interval</td>
<td>The maximum query response time advertised in IGMPv2 queries.</td>
</tr>
<tr>
<td>Robust Count</td>
<td>Displays the number of times the router will retry a query.</td>
</tr>
</tbody>
</table>

Sample Output

*A:ALA-BA# show router 100 igmp status
===============================================================================
IGMP Status
===============================================================================
| Admin State      | Up                                          |
| Oper State       | Up                                          |
| Query Interval   | 1024                                         |
| Last Member Query Interval | 1024                                         |
| Query Response Interval | 1023                                         |
| Robust Count     | 10                                          |
===============================================================================
*A:ALA-BA#
Show Router PIM Commands

anycast

Syntax  anycast [detail]
Context  show>router>pim

Description  This command displays PIM anycast rp-set information.

Parameters  
- detail — Displays detailed information.

Output  PIM anycast Output — The following table provides PIM anycast field descriptions

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anycast Address</td>
<td>Displays the candidate anycast address.</td>
</tr>
<tr>
<td>Anycast RP Peer</td>
<td>Displays the candidate anycast RP peer address.</td>
</tr>
</tbody>
</table>

Sample Output

A:dut-d# show router pim anycast

PIM Anycast RP Entries

<table>
<thead>
<tr>
<th>Anycast RP</th>
<th>Anycast RP Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>100.100.100.1</td>
<td>102.1.1.1</td>
</tr>
<tr>
<td>103.1.1.1</td>
<td>104.1.1.1</td>
</tr>
</tbody>
</table>

PIM Anycast RP Entries : 3

---

crp

Syntax  crp [ip-address]
Context  show>router>pim

Description  Display PIM candidate RP (CRP) information received at the elected Bootstrap router (BSR).

Parameters  
- ip-address — The candidate RP IP address.
### PIM CRP Output —

The following table provides PIM CRP field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP Address</td>
<td>Displays the Candidate RP address.</td>
</tr>
<tr>
<td>Group Address</td>
<td>Displays the range of multicast group addresses for which the CRP is the Candidate RP.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the Candidate RP's priority for becoming a rendezvous point (RP). This value is used to elect RP for a group range. A value of 0 is considered as the highest priority.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Displays the hold time of the candidate RP. It is used by the Bootstrap router to time out the RP entries if it does not listen to another CRP advertisement within the holdtime period.</td>
</tr>
<tr>
<td>Expiry</td>
<td>The minimum time remaining before the CRP will be declared down. If the local router is not the BSR, this value is 0.</td>
</tr>
<tr>
<td>Candidate RPs</td>
<td>Displays the number of CRP entries.</td>
</tr>
</tbody>
</table>

### Sample Output

A:WAS# show router pim crp

```
PIM Candidate RPs
RP Address Group Address Priority Holdtime Expiry Time
2.22.187.236 224.0.0.0/4 192 150 0d 00:02:19
2.22.187.239 224.0.0.0/4 192 150 0d 00:02:19
2.22.187.240 224.0.0.0/4 192 150 0d 00:02:09
```

Candidate RPs : 3

A:WAS#

A:WAS# show router pim crp 2.22.187.236

```
PIM Candidate RPs
RP Address Group Address Priority Holdtime Expiry Time
2.22.187.236 224.0.0.0/4 192 150 0d 00:01:43
```

Candidate RPs : 1

A:WAS#
s-pmsi

Syntax  s-pmsi [mdSrcAddr [mdGrpAddr]] [detail]

Context  show>router>pim

Description  Displays the list of selective provider multicast service interfaces that are currently active.

Parameters  

mdSrcAddr — Specifies the source address of the multicast sender.

mdGrpAddr — Specifies the group address of the multicast sender.

detail — Displays detailed output.

Output  PIM data MDT Output — The following table provides PIM data MDT descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MD Grp Address</td>
<td>Displays the IP multicast group address for which this entry contains information.</td>
</tr>
<tr>
<td>MD Src Address</td>
<td>Displays the source address of the multicast sender. It will be 0 if the type is configured as starg. It will be the address of the Rendezvous Point (RP) if the type is configured as starRP.</td>
</tr>
<tr>
<td>MT Index</td>
<td>Displays the index number.</td>
</tr>
<tr>
<td>Num VP SGs</td>
<td>Displays the VPN number.</td>
</tr>
</tbody>
</table>

Sample Output

*B:node-6# show router 100 pim s-pmsi

PIM Selective provider tunnels

<table>
<thead>
<tr>
<th>MD Src Address</th>
<th>MD Grp Address</th>
<th>MT Index</th>
<th>Num VPN SGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.72</td>
<td>24603</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.73</td>
<td>24604</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.74</td>
<td>24605</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.75</td>
<td>24606</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.76</td>
<td>24607</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.77</td>
<td>24608</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.78</td>
<td>24609</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.79</td>
<td>24610</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.80</td>
<td>24611</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.81</td>
<td>24612</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.82</td>
<td>24613</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.83</td>
<td>24614</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.84</td>
<td>24615</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.85</td>
<td>24616</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.86</td>
<td>24617</td>
<td>1</td>
</tr>
<tr>
<td>200.200.200.7</td>
<td>230.0.89.87</td>
<td>24618</td>
<td>1</td>
</tr>
</tbody>
</table>

*B:node-6#
group

Syntax  
group grp-ip-address [source ip-address] [type {starstarrp | starg | sg}] [detail] [family]

Context  
show>router>pim

Description  
This command displays PIM source group database information.

Parameters

grp-ip-address — Specifies the IP multicast group address for which this entry contains information.

source ip-address — Specifies the source address for which this entry contains information.

type starstarrp — Specifies that only (*, *, rp) entries be displayed.
**IGMP Commands**

*type starg* — Specifies that only \((*,G)\) entries be displayed.

*type sg* — specifies that only \((S,G)\) entries be displayed.

*detail* — Displays detailed group information.

*family* — Displays either IPv4 or IPv6 information.

**Output**  
**PIM Group Output** — The following table provides PIM Group field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Displays the IP multicast group address for which this entry contains information.</td>
</tr>
<tr>
<td>Source Address</td>
<td>Displays the source address of the multicast sender. It will be 0 if the type is configured as starg. It will be the address of the Rendezvous Point (RP) if the type is configured as starRP.</td>
</tr>
<tr>
<td>RP Address</td>
<td>Displays the RP address.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the type of entry, ((<em>,</em>, rp)/(*,G)) or ((S,G)).</td>
</tr>
<tr>
<td>Spt Bit</td>
<td>Specifies whether to forward on ((<em>,</em>, rp)/(*,G)) or on ((S,G)) state. It is updated when the ((S,G)) data comes on the RPF interface towards the source.</td>
</tr>
<tr>
<td>Incoming Intf</td>
<td>Displays the interface on which the traffic comes in. It can be the RPF interface to the RP (if starg) or the source (if sg).</td>
</tr>
<tr>
<td>Num Oifs</td>
<td>Displays the number of interfaces in the inherited outgoing interface list. An inherited list inherits the state from other types.</td>
</tr>
<tr>
<td>Flags</td>
<td>Displays the different lists that this interface belongs to.</td>
</tr>
<tr>
<td>Keepalive Timer Exp</td>
<td>The keepalive timer is applicable only for ((S,G)) entries. The ((S,G)) keepalive timer is updated by data being forwarded using this ((S,G)) Forwarding state. It is used to keep ((S,G)) state alive in the absence of explicit ((S,G)) joins.</td>
</tr>
<tr>
<td>MRIB Next Hop</td>
<td>Displays the next hop address towards the RP.</td>
</tr>
<tr>
<td>MRIB Src Flags</td>
<td>Displays the MRIB information about the source. If the entry is of type starg or starstarpp, it will contain information about the RP for the group.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Displays the time since this source group entry was created.</td>
</tr>
<tr>
<td>Resolved By</td>
<td>Displays the route table used for RPF check.</td>
</tr>
<tr>
<td>Up JP State</td>
<td>Displays the upstream join prune state for this entry on the interface. PIM join prune messages are sent by the downstream routers towards the RPF neighbor.</td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Up JP Expiry</td>
<td>Displays the minimum amount of time remaining before this entry will be aged out.</td>
</tr>
<tr>
<td>Up JP Rpt</td>
<td>Displays the join prune Rpt state for this entry on the interface. PIM join/prune messages are sent by the downstream routers towards the RPF neighbor. (S,G, rpt) state is a result of receiving (S,G, rpt) JP message from the downstream router on the RP tree.</td>
</tr>
<tr>
<td>Up JP Rpt Over-ride</td>
<td>Displays the value used to delay triggered Join (S,G, rpt) messages to prevent implosions of triggered messages. If this has a non-zero value, it means that the router was in 'notPruned' state and it saw a prune (S,G, rpt) message being sent to RPF (S,G, rpt). If the router sees a join (S,G, rpt) override message being sent by some other router on the LAN while the timer is still non-zero, it simply cancels the override timer. If it does not see a join (S,G, rpt) message, then on expiry of the override timer, it sends its own join (S,G, rpt) message to RPF (S,G, rpt). A similar scenario exists when RPF (S,G, rpt) changes to become equal to RPF (*,G).</td>
</tr>
<tr>
<td>Register State</td>
<td>Specifies the register state. The register state is kept at the source DR. When the host starts sending multicast packets and if there are no entries programmed for that group, the source DR sends a register packet to the RP (g). Register state transition happen based on the register stop timer and the response received from the RP.</td>
</tr>
<tr>
<td>Register Stop Exp</td>
<td>Displays the time remaining before the register state might transition to a different state.</td>
</tr>
<tr>
<td>Register from Anycast RP</td>
<td>Displays if the register packet for that group has been received from one of the RP from the anycast-RP set.</td>
</tr>
<tr>
<td>RPF Neighbor</td>
<td>Displays the address of the RPF neighbor.</td>
</tr>
<tr>
<td>Outgoing Intf List</td>
<td>Displays a list of interfaces on which data is forwarded.</td>
</tr>
<tr>
<td>Curr Fwding Rate</td>
<td>Displays the current forwarding rate of the multicast data for this group and source.</td>
</tr>
<tr>
<td>Forwarded Packets</td>
<td>Displays the number of multicast packets that were forwarded to the interfaces in the outgoing interface list.</td>
</tr>
<tr>
<td>Discarded Packets</td>
<td>Displays the number of multicast packets that matched this source group entry but were discarded. For (S,G) entries, if the traffic is getting forwarded on the SPT, the packets arriving from the RPT will be discarded.</td>
</tr>
<tr>
<td>Forwarded Octets</td>
<td>Displays the number of octets forwarded.</td>
</tr>
<tr>
<td>RPF Mismatches</td>
<td>Displays the number of multicast packets that matched this source group entry but they did not arrive on the interface.</td>
</tr>
</tbody>
</table>
Sample Output

A:NYC>show>router>pim# group

PIM Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>RP Address</th>
<th>Type</th>
<th>Spt Incoming</th>
<th>Num</th>
<th>Bit Intf</th>
<th>Oifs</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.24.24.24</td>
<td>*</td>
<td>2.22.187.240</td>
<td>&lt;*,G&gt;</td>
<td>nyc-sjc</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>239.255.255.250</td>
<td>*</td>
<td>2.22.187.240</td>
<td>&lt;*,G&gt;</td>
<td>nyc-sjc</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Groups : 2

A:NYC>show>router>pim#

A:NYC>show>router>pim# group 239.255.255.250

PIM Groups

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>RP Address</th>
<th>Type</th>
<th>Spt Incoming</th>
<th>Num</th>
<th>Bit Intf</th>
<th>Oifs</th>
</tr>
</thead>
<tbody>
<tr>
<td>239.255.255.250</td>
<td>*</td>
<td>2.22.187.240</td>
<td>&lt;*,G&gt;</td>
<td>nyc-sjc</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Groups : 1

A:NYC>show>router>pim#

A:NYC>show>router>pim# group 239.255.255.250 detail

PIM Source Group

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>RP Address</th>
<th>Type</th>
<th>Keepalive Timer Exp:</th>
<th>MRIB Next Hop</th>
<th>MRIB Src Flags</th>
<th>Up Time</th>
<th>Resolved By</th>
<th>Up JP State</th>
<th>MRIB Next Hop</th>
<th>MRIB Src Flags</th>
<th>Up JP Rpt Override</th>
<th>Register State</th>
<th>Register Stop Exp</th>
<th>Reg From Anycast RP</th>
<th>UP Fwding Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>239.255.255.250</td>
<td>16.1.1.2</td>
<td>100.100.100.1</td>
<td>(S,G)</td>
<td>0d 00:03:07</td>
<td>16.1.1.2</td>
<td>direct</td>
<td>0d 00:50</td>
<td>rtable-u</td>
<td>Joined</td>
<td>16.1.1.2</td>
<td>direct</td>
<td>0d 00:00:00</td>
<td>Pruned</td>
<td>0d 00:00:47</td>
<td>No</td>
<td>482.9 kbps</td>
</tr>
</tbody>
</table>
Forwarded Packets : 1262  Discarded Packets : 0
Forwarded Octets  : 1269572  RPF Mismatches : 0
Spt threshold    : 0 kbps

A:NYC>show>router>pim#

B:Dut-C# show router pim group 225.0.0.1 type sg detail

PIM Source Group ipv4

Group Address      : 225.0.0.1
Source Address     : 11.11.0.1
RP Address         : 10.20.1.3
Flags              : rpt-prn-des
MRIB Next Hop      : 11.11.0.1
MRIB Src Flags     : direct
Up Time            : 0d 00:04:17
Resolved By        : rtable-u
Up JP State        : Joined
Up JP Expiry       : 0d 00:00:00
Up JP Rpt          : Pruned
Up JP Rpt Override : 0d 00:00:00
Register State     : No Info
Reg From Anycast RP: No
Rpf Neighbor       : 11.11.0.1
Incoming Intf      : svc_itf
Outgoing Host List : 112.112.1.1
Curr Fwding Rate   : 0.0 kbps
Forwarded Packets  : 0  Discarded Packets : 0
Forwarded Octets   : 0  RPF Mismatches : 0
Spt threshold      : 0 kbps
ECMP opt threshold : 7
Admin bandwidth    : 1 kbps
Prefernece         : 0

PIM Source Group ipv4

Group Address      : 225.0.0.1
Source Address     : 11.11.0.2
RP Address         : 10.20.1.3
Flags              :            Type : (S,G)
MRIB Next Hop      : 11.11.0.2
MRIB Src Flags     : direct
Up Time            : 0d 00:04:18
Resolved By        : rtable-u
Up JP State        : Joined
Up JP Expiry       : 0d 00:00:00
Up JP Rpt          : Not Pruned
Up JP Rpt Override : 0d 00:00:00
Register State     : No Info
Reg From Anycast RP: No
Rpf Neighbor       : 11.11.0.2
Incoming Intf      : svc_itf
Outgoing Host List : 112.112.1.1, 112.112.1.2
Curr Fwding Rate   : 0.0 kbps
Forwarded Packets  : 0  Discarded Packets : 0
Forwarded Octets   : 0  RPF Mismatches : 0
IGMP Commands

```
Spt threshold : 0 kbps    ECMP opt threshold : 7
Admin bandwidth : 1 kbps   Preference   : 0
-------------------------------------------------------------------
Groups : 2
-------------------------------------------------------------------
*B:Dut-C#
```

**interface**

**Syntax**
```
interface [ip-int-name | mt-int-name | ip-address] [group grp-ip-address | source ip-address [type {starstarrp | starg | sg}] [detail] [family]
```

**Context**
```
show>router>pim
```

**Description**
This command displays PIM interface information and the (S,G)/(*,G)/(*, *, rp) state of the interface.

**Parameters**
- `ip-int-name` — Only displays the interface information associated with the specified IP interface name.
- `ip-address` — Only displays the interface information associated with the specified IP address.
- `group grp-ip-address` — Specifies the IP multicast group address for which this entry contains information.
- `source ip-address` — Specifies the source address for which this entry contains information.
  
  If the type is starg, the value of this object will be zero.
  
  If the type is starstarrp, the value of this object will be address of the RP.
- `type` — Specifies the type of this entry.
  
  **Values**
  - `starstarrp`, `starg`, `sg`
- `detail` — Displays detailed interface information.
- `family` — Displays IPv4 or IPv6 information for the interface.

**Output**

**PIM Interface Output** — The following table provides PIM interface field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Displays the administrative state for PIM protocol on this interface.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Displays the current operational state of PIM protocol on this interface.</td>
</tr>
<tr>
<td>DR</td>
<td>Displays the designated router on this PIM interface.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>Displays the priority value sent in PIM Hello messages and that is used by routers to elect the designated router (DR).</td>
</tr>
<tr>
<td>Hello Intvl</td>
<td>Indicates the frequency at which PIM Hello messages are transmitted on this interface.</td>
</tr>
</tbody>
</table>
Sample Output

ALA-1# show router pim interface

PIM Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>DR</th>
<th>DR Priority</th>
<th>Hello Intvl</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>Up</td>
<td>Up</td>
<td>N/A</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>ip-10.1.7.1</td>
<td>Up</td>
<td>Up</td>
<td>10.1.7.7</td>
<td>5</td>
<td>30</td>
</tr>
<tr>
<td>ip-10.1.2.1</td>
<td>Up</td>
<td>Up</td>
<td>10.1.2.2</td>
<td>5</td>
<td>30</td>
</tr>
<tr>
<td>ip-100.111.1.1</td>
<td>Up</td>
<td>Up</td>
<td>100.111.1.1</td>
<td>5</td>
<td>30</td>
</tr>
</tbody>
</table>

Interfaces : 4

ALA-1#

ALA-1# show router pim interface ip-10.1.2.1 detail

PIM Interface ip-10.1.2.1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>DR</th>
<th>DR Priority</th>
<th>Hello Intvl</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-10.1.2.1</td>
<td>Up</td>
<td>Up</td>
<td>10.1.2.2</td>
<td>5</td>
<td>30</td>
</tr>
</tbody>
</table>

PIM Group Source

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>RP Address</th>
<th>Type</th>
<th>JP</th>
<th>Assert</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.101.0.5</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.1</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.2</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.3</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
</tbody>
</table>

ALA-1#

ALA-1# show router pim interface group

PIM Interface ip-10.1.7.1

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>DR</th>
<th>DR Priority</th>
<th>Hello Intvl</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-10.1.7.1</td>
<td>Up</td>
<td>Up</td>
<td>10.1.7.7</td>
<td>5</td>
<td>30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>RP Address</th>
<th>Type</th>
<th>JP</th>
<th>Assert</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.101.0.0</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.1</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.2</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.3</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>IP Address</td>
<td>Source Address</td>
<td>RP Address</td>
<td>Type</td>
<td>JP</td>
<td>Assert</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>------------</td>
<td>------</td>
<td>----</td>
<td>--------</td>
</tr>
<tr>
<td>228.101.0.4</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.6</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.7</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.8</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.101.0.9</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Interface ip-10.1.2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>ip-10.1.2.1</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>RP Address</th>
<th>Type</th>
<th>JP</th>
<th>Assert</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.101.0.5</td>
<td>100.111.1.2</td>
<td>200.200.200.4</td>
<td>&lt;S,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Interface ip-100.111.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>ip-100.111.1.1</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Source Address</th>
<th>RP Address</th>
<th>Type</th>
<th>JP</th>
<th>Assert</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.102.0.0</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.1</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.2</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.3</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.4</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.5</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.6</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.7</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.8</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
<tr>
<td>228.102.0.9</td>
<td>*</td>
<td>200.200.200.4</td>
<td>&lt;*,G&gt;</td>
<td>Join</td>
<td>No Info</td>
</tr>
</tbody>
</table>

---

Interfaces : 3

ALA-1# show router pim interface group 228.102.0.0 detail

**PIM Interface ip-100.111.1.1**

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>DR</th>
<th>Priority</th>
<th>Hello Intvl</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-100.111.1.1</td>
<td>Up</td>
<td>Up</td>
<td>100.111.1.1</td>
<td>5</td>
<td>30</td>
</tr>
</tbody>
</table>

**PIM Group Source**

- **Group Address**: 228.102.0.0
- **Src Address**: *
- **Interface**: ip-100.111.1.1
- **Type**: <*,G>
- **RP Address**: 200.200.200.4
- **Join Prune State**: Join
- **Expires**: 0d 00:02:05
- **Prune Pend Expires**: N/A
Display of Multicast routing interface information:

```
Assert State       : No Info
-------------------------------------------------------------------------------
Interfaces : 1
-------------------------------------------------------------------------------

ALA-1# show router pim interface type starg

PIM Interface ip-100.111.1.1
Interface          : ip-100.111.1.1
Admin  Oper   DR              DR        Hello  
State  State                  Priority  Intvl
-------------------------------------------------------------------------------
ip-100.111.1.1                  Up     Up     100.111.1.1     5         30
-------------------------------------------------------------------------------

Group Address    Source Address   RP Address       Type     JP        Assert
-------------------------------------------------------------------------------
228.102.0.0      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.1      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.2      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.3      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.4      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.5      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.6      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.7      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.8      *                200.200.200.4    <*,G>    Join      No Info
228.102.0.9      *                200.200.200.4    <*,G>    Join      No Info

Interfaces : 1
-------------------------------------------------------------------------------

ALA-1# show router pim interface detail

PIM Interface int1
Interface          : int1
Admin Status       : Up                 Oper Status        : Up
DR                 : 10.1.1.1           Oper DR Priority   : 1
BSM RA Check       : Disabled           Cfg DR Priority    : 1
Hello Interval     : 30                 Time for next hello: 0d 00:00:23
Multicast Senders  : auto               Hello Multiplier   : 35
J/P Tracking Admin : Disabled           J/P Tracking Oper  : Disabled
Auto-created       : No                 Improved Assert    : Enabled
Sticky-DR          : Disabled           Sticky-DR Priority : N/A
Max Groups Allowed : 0                  Max Groups Till Now: 0
Num Groups         : 0                  Bfd Enabled        : No
-------------------------------------------------------------------------------

PIM Interface sender
Interface          : sender
Admin Status       : Up                 Oper Status        : Up
DR                 : 11.1.1.1           Oper DR Priority   : 1
-------------------------------------------------------------------------------

A:SetupCLI# show router pim interface detail

PIM Interface int1
Interface          : int1
Admin Status       : Up                 Oper Status        : Up
DR                 : 10.1.1.1           Oper DR Priority   : 1
BSM RA Check       : Disabled           Cfg DR Priority    : 1
Hello Interval     : 30                 Time for next hello: 0d 00:00:23
Multicast Senders  : auto               Hello Multiplier   : 35
J/P Tracking Admin : Disabled           J/P Tracking Oper  : Disabled
Auto-created       : No                 Improved Assert    : Enabled
Sticky-DR          : Disabled           Sticky-DR Priority : N/A
Max Groups Allowed : 0                  Max Groups Till Now: 0
Num Groups         : 0                  Bfd Enabled        : No
-------------------------------------------------------------------------------

PIM Interface sender
Interface          : sender
Admin Status       : Up                 Oper Status        : Up
DR                 : 11.1.1.1           Oper DR Priority   : 1
-------------------------------------------------------------------------------

A:SetupCLI#```
neighbor

**Syntax**
```
neighbor [ip-address | ip-int-name [address ip-address]] [detail] [family]
```

**Context**
```
show>router>pim
```

**Description**
This command displays PIM neighbor information.

This can be important if an interface has more than one adjacency. For example, a LAN-interface configuration with three routers connected and all are running PIM on their LAN interfaces. These routers then have two adjacencies on their LAN interface, each with different neighbors. If the `address` parameter is not defined in this example, then the `show` command output would display two adjacencies.

**Parameters**
- `neighbor ip-int-name` — Only displays the interface information associated with the specified IP interface name.
- `neighbor ip-address` — Only displays the interface information associated with the specified IP address.
- `address ip-address` — The IP address of the neighbor, on the other side of the interface.
- `detail` — Displays detailed neighbor information.
- `family` — Displays either IPv4 or IPv6 information for the specified neighbor.

**Output**

**PIM Neighbor Output** — The following table provides PIM neighbor field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the neighbor’s interface name.</td>
</tr>
<tr>
<td>Nbr DR Priority</td>
<td>Displays the value of the neighbor's DR priority which is received in the hello message.</td>
</tr>
<tr>
<td>Nbr Address</td>
<td>Displays the neighbor’s address.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Displays the time since this PIM neighbor (last) became a neighbor of the local router.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Displays the minimum time remaining before this PIM neighbor will be aged out.</td>
</tr>
<tr>
<td></td>
<td>0 — Means that this neighbor will never be aged out. This happens when the PIM neighbor sends a Hello message with holdtime set to '0xffff'.</td>
</tr>
<tr>
<td>Hold Time</td>
<td>Displays the value of the hold time present in the hello message.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>Displays the value of the neighbor's DR priority which is received in the hello message.</td>
</tr>
<tr>
<td>Tracking Support</td>
<td>Displays whether the T bit in the LAN prune delay option was present in the hello message. This indicates the neighbor's capability to disable join message suppression.</td>
</tr>
<tr>
<td>LAN Delay</td>
<td>Displays the value of the LAN delay field present in the hello message received from the neighbor.</td>
</tr>
</tbody>
</table>
### Sample Output

ALA-1# show router pim neighbor

<table>
<thead>
<tr>
<th>Interface</th>
<th>Nbr DR Priority</th>
<th>Nbr Address</th>
<th>Up Time</th>
<th>Expiry Time</th>
<th>Hold Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-10.1.7.1</td>
<td>5</td>
<td>10.1.7.7</td>
<td>0d 00:10:39</td>
<td>0d 00:01:36</td>
<td>105</td>
</tr>
<tr>
<td>ip-10.1.2.1</td>
<td>5</td>
<td>10.1.2.2</td>
<td>0d 00:10:39</td>
<td>0d 00:01:35</td>
<td>105</td>
</tr>
<tr>
<td>ip-100.111.1.1</td>
<td>3</td>
<td>100.111.1.2</td>
<td>0d 00:09:31</td>
<td>0d 00:01:15</td>
<td>105</td>
</tr>
</tbody>
</table>

Neighbors : 3

ALA-1#

ALA-1# show router pim neighbor detail

<table>
<thead>
<tr>
<th>Interface</th>
<th>Neighbor Addr</th>
<th>DR Priority</th>
<th>LAN Delay(ms)</th>
<th>Override Intvl(ms)</th>
<th>Gen Id</th>
<th>Up Time</th>
<th>Expiry Time</th>
<th>Hold Time(sec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-10.1.7.1</td>
<td>10.1.7.7</td>
<td>5</td>
<td>500</td>
<td>2500</td>
<td>26470</td>
<td>0d 00:10:41</td>
<td>0d 00:01:34</td>
<td>105</td>
</tr>
<tr>
<td>ip-10.1.2.1</td>
<td>10.1.2.2</td>
<td>5</td>
<td>500</td>
<td>2500</td>
<td>37928</td>
<td>0d 00:10:42</td>
<td>0d 00:01:33</td>
<td>105</td>
</tr>
</tbody>
</table>

### Description (Continued)

**Gen Id**

Displays a randomly generated 32-bit value that is regenerated each time PIM forwarding is started or restarted on the interface, including when the router itself restarts. When a hello message with a new GenID is received from a neighbor, any old hello information about that neighbor is discarded and superseded by the information from the new hello message.

**Override Intvl (ms)**

Displays the value of the override interval present in the Hello message.
IGMP Commands

Interface : ip-100.111.1.1
Neighbor Addr : 100.111.1.2  DR Priority : 3
Tracking Support : No  LAN Delay(ms) : 500
Gen Id : 742098371  Override Intvl(ms) : 2500
Up Time : 0d 00:09:33  Expiry Time : 0d 00:01:43
Hold Time/sec : 105

Neighbors : 3

ALa-1#

rp

Syntax rp ip-address

Context show>router>pim

Description This command displays the rendezvous point (RP) set information built by the router.

Parameters ip-address — Specifies the IP address of the RP.

Output PIM Neighbor Output — The following table provides PIM neighbor field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Displays the multicast group address of the entry.</td>
</tr>
<tr>
<td>RP Address</td>
<td>Displays the address of the Rendezvous Point (RP).</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the entry was learned through the Bootstrap mechanism or if it was statically configured.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the priority for the specified group address. The higher the value, the higher the priority.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Displays the value of the hold time present in the BSM message.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALa-1# show router pim rp

PIM RP Set

<table>
<thead>
<tr>
<th>Group Address</th>
<th>RP Address</th>
<th>Type</th>
<th>Priority</th>
<th>Holdtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.0/4</td>
<td>200.200.200.4</td>
<td>Dynamic</td>
<td>192</td>
<td>150</td>
</tr>
<tr>
<td>10.1.7.1</td>
<td>Static</td>
<td>1</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Group Prefixes : 1

A:ALa-1#

A:ALa-1# show router pim rp 10.1.7.1
PIM RP Set

<table>
<thead>
<tr>
<th>Group Address</th>
<th>RP Address</th>
<th>Type</th>
<th>Priority</th>
<th>Holdtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.0/4</td>
<td>10.1.7.1</td>
<td>Static</td>
<td>1</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Group Prefixes : 1

A:ALA-1#

rp-hash

**Syntax**

rp-hash grp-ip-address

**Context**

show>router>pim

**Description**

This command hashes the RP for the specified group from the RP set.

**Parameters**

 grp-ip-address — Displays specific multicast group addresses.

**Output**

PIM RP-Hash Output — The following table provides RP-Hash output field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Displays the multicast group address of the entry.</td>
</tr>
<tr>
<td>RP Address</td>
<td>Displays the address of the Rendezvous Point (RP).</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the entry was learned through the Bootstrap mechanism or if it was statically configured.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
A:ALA-1# show router pim rp-hash 228.101.0.0
PIM Group-To-RP mapping
<table>
<thead>
<tr>
<th>Group Address</th>
<th>RP Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.101.0.0</td>
<td>200.200.200.4</td>
<td>Bootstrap</td>
</tr>
</tbody>
</table>
```

```
A:ALA-1# show router pim rp-hash 228.101.0.6
PIM Group-To-RP mapping
<table>
<thead>
<tr>
<th>Group Address</th>
<th>RP Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.101.0.6</td>
<td>200.200.200.4</td>
<td>Bootstrap</td>
</tr>
</tbody>
</table>
```

A:ALA-1#
IGMP Commands

statistics

Syntax  statistics [ip-int-name | mt-int-name | ip-address] [family]

Context  show>router>pim

Description  This command displays statistics for a particular PIM instance.

Parameters  ip-int-name — Only displays the interface information associated with the specified IP interface name.

ip-address — Only displays the interface information associated with the specified IP address.

family — Displays either IPv4 or IPv6 information.

Output  PIM Statistics Output — The following table provides PIM statistics output field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM Statistics</td>
<td>The section listing the PIM statistics for a particular interface.</td>
</tr>
<tr>
<td>Message Type</td>
<td>Displays the type of message.</td>
</tr>
<tr>
<td>Hello</td>
<td>Displays the number of PIM hello messages received or transmitted on this interface.</td>
</tr>
<tr>
<td>Join Prune</td>
<td>Displays the number of PIM join prune messages received or transmitted on this interface.</td>
</tr>
<tr>
<td>Asserts</td>
<td>Displays the number of PIM assert messages received or transmitted on this interface.</td>
</tr>
<tr>
<td>Register</td>
<td>Displays the number of register messages received or transmitted on this interface.</td>
</tr>
<tr>
<td>Null Register</td>
<td>Displays the number of PIM null register messages received or transmitted on this interface.</td>
</tr>
<tr>
<td>Register Stop</td>
<td>Displays the number of PIM register stop messages received or transmitted on this interface.</td>
</tr>
<tr>
<td>BSM</td>
<td>Displays the number of PIM Bootstrap messages (BSM) received or transmitted on this interface.</td>
</tr>
<tr>
<td>Candidate RP Adv</td>
<td>Displays the number of candidate RP advertisements.</td>
</tr>
<tr>
<td>Total Packets</td>
<td>Displays the total number of packets transmitted and received on this interface.</td>
</tr>
<tr>
<td>Received</td>
<td>Displays the number of messages received on this interface.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Displays the number of multicast data packets transmitted on this interface.</td>
</tr>
<tr>
<td>Rx Errors</td>
<td>Displays the total number of receive errors.</td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>General Interface Statistics</td>
<td>The section listing the general PIM interface statistics.</td>
</tr>
<tr>
<td>Register TTL Drop</td>
<td>Displays the number of multicast data packets which could not be encapsulated in Register messages because the time to live (TTL) was zero.</td>
</tr>
<tr>
<td>Tx Register MTU Drop</td>
<td>Displays the number of Bootstrap messages received on this interface but were dropped.</td>
</tr>
<tr>
<td>Rx Invalid Register</td>
<td>Displays the number of invalid PIM register messages received on this interface.</td>
</tr>
<tr>
<td>Rx Neighbor Unknown</td>
<td>Displays the number of PIM messages (other than hello messages) which were received on this interface and were rejected because the adjacency with the neighbor router was not already established.</td>
</tr>
<tr>
<td>Rx Bad Checksum Discard</td>
<td>Displays the number of PIM messages received on this interface which were discarded because of bad checksum.</td>
</tr>
<tr>
<td>Rx Bad Encoding</td>
<td>Displays the number of PIM messages with bad encodings received on this interface.</td>
</tr>
<tr>
<td>Rx Bad Version Discard</td>
<td>Displays the number of PIM messages with bad versions received on this interface.</td>
</tr>
<tr>
<td>Rx CRP No Router Alert</td>
<td>Displays the number of candidate-rp advertisements (C-RP-Adv) received on this interface which had no router alert option set.</td>
</tr>
<tr>
<td>Rx Invalid Join Prune</td>
<td>Displays the number of invalid PIM join prune messages received on this interface.</td>
</tr>
<tr>
<td>Rx Unknown PDU Type</td>
<td>Displays the number of packets received with an unsupported PIM type.</td>
</tr>
<tr>
<td>Join Policy Drops</td>
<td>Displays the number of times the join policy match resulted in dropping PIM join-prune message or one of the source group contained in the message.</td>
</tr>
<tr>
<td>Register Policy Drops</td>
<td>Displays the number of times the register policy match resulted in dropping PIM register message.</td>
</tr>
<tr>
<td>Bootstrap Import Policy Drops</td>
<td>Displays the number of Bootstrap messages received on this interface but were dropped because of Bootstrap import policy.</td>
</tr>
<tr>
<td>Bootstrap Export Policy Drops</td>
<td>Displays the number of Bootstrap messages that were not transmitted on this interface because of Bootstrap export policy.</td>
</tr>
<tr>
<td>Source Group Statistics</td>
<td>The section listing the source group statistics.</td>
</tr>
<tr>
<td>((S,G))</td>
<td>Displays the number of entries in which the type is ((S,G)).</td>
</tr>
</tbody>
</table>
Sample output

A:ALA-1# show router pim statistics

PIM Statistics

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Received</th>
<th>Transmitted</th>
<th>Rx Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>198</td>
<td>200</td>
<td>0</td>
</tr>
<tr>
<td>Join Prune</td>
<td>96</td>
<td>75</td>
<td>0</td>
</tr>
<tr>
<td>Asserts</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Register</td>
<td>0</td>
<td>30</td>
<td>0</td>
</tr>
<tr>
<td>Null Register</td>
<td>0</td>
<td>160</td>
<td>0</td>
</tr>
<tr>
<td>Register Stop</td>
<td>180</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BSM</td>
<td>34</td>
<td>76</td>
<td>0</td>
</tr>
<tr>
<td>Candidate RP Adv</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total Packets</td>
<td>546</td>
<td>541</td>
<td></td>
</tr>
</tbody>
</table>

General Interface Statistics

<table>
<thead>
<tr>
<th>Description</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register TTL Drop</td>
<td>0</td>
</tr>
<tr>
<td>Tx Register MTU Drop</td>
<td>0</td>
</tr>
<tr>
<td>Rx Invalid Register</td>
<td>0</td>
</tr>
<tr>
<td>Rx Neighbor Unknown</td>
<td>0</td>
</tr>
<tr>
<td>Rx Bad Checksum Discard</td>
<td>0</td>
</tr>
<tr>
<td>Rx Bad Encoding</td>
<td>0</td>
</tr>
<tr>
<td>Rx Bad Version Discard</td>
<td>0</td>
</tr>
<tr>
<td>Rx CRP No Router Alert</td>
<td>0</td>
</tr>
<tr>
<td>Rx Unknown PDU Type</td>
<td>0</td>
</tr>
<tr>
<td>Join Policy Drops</td>
<td>0</td>
</tr>
<tr>
<td>Register Policy Drops</td>
<td>0</td>
</tr>
<tr>
<td>Bootstrap Import Policy Drops</td>
<td>0</td>
</tr>
<tr>
<td>Bootstrap Export Policy Drops</td>
<td>0</td>
</tr>
</tbody>
</table>

Source Group Statistics

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S,G)</td>
<td>10</td>
</tr>
<tr>
<td>(*.G)</td>
<td>10</td>
</tr>
<tr>
<td>(<em>.</em>,RP)</td>
<td>0</td>
</tr>
</tbody>
</table>

A:ALA-1# show router pim statistics 10.1.7.1

PIM Interface 10.1.7.1 Statistics

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Received</th>
<th>Transmitted</th>
<th>Rx Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>62</td>
<td>66</td>
<td>0</td>
</tr>
<tr>
<td>Join Prune</td>
<td>36</td>
<td>21</td>
<td>0</td>
</tr>
</tbody>
</table>

Displays the number of entries in which the type is (*.G).

Displays the number of entries in which the type is (*. *, rp).
### Multicast

| Asserts | 0 | 0 | 0 |
| Register | 0 | 0 | 0 |
| Null Register | 0 | 0 | 0 |
| Register Stop | 0 | 0 | 0 |
| BSM | 33 | 3 | 0 |
| Total Packets | 134 | 90 |

---

**General Interface Statistics**

---

**Interface Source Group Statistics**

---

```
A:ALA-1#
A:ALA-1# show router pim statistics ip-10.1.7.1
```

---

**PIM Interface ip-10.1.7.1 Statistics**

---

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Received</th>
<th>Transmitted</th>
<th>Rx Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello</td>
<td>63</td>
<td>67</td>
<td>0</td>
</tr>
<tr>
<td>Join Prune</td>
<td>36</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>Asserts</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Null Register</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Register Stop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>BSM</td>
<td>33</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Total Packets</td>
<td>135</td>
<td>91</td>
<td></td>
</tr>
</tbody>
</table>

---

**General Interface Statistics**

---

```
A:ALA-1#
```
Join Policy Drops                 : 0
Register Policy Drops             : 0
Bootstrap Import Policy Drops     : 0
Bootstrap Export Policy Drops     : 0

----------------------------------------------------------------

Interface Source Group Statistics
----------------------------------------------------------------
(S,G)                             : 9
(*,G)                             : 0
(*,*,RP)                          : 0

================================================================

A:ALA-1#

status

Syntax    status [detail] [family]
Context   show>router>pim

Description
This command displays PIM status. The Oper Status reflects the combined operational status of IPv4/IPv6 PIM protocol status. If both are down, then Oper Status will be reflected as down. If IPv4 or IPv6 reflects up, the Oper Status will reflect up.

If PIM is not enabled, the following message appears:

A:NYC# show router pim status
MINOR: CLI PIM is not configured.
A:NYC#

Parameters

detail — Displays detailed status information.

family — Displays either IPv4 or IPv6 information.

Output

PIM Status Output — The following table provides PIM status output field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Displays the administrative status of PIM.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Displays the current operating state of this PIM protocol instance.</td>
</tr>
<tr>
<td>BSR State</td>
<td>Displays the state of the router with respect to the Bootstrap mechanism.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the address of the elected Bootstrap router.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Displays the time remaining before the router sends the next Bootstrap message.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the priority of the elected Bootstrap router. The higher the value, the higher the priority.</td>
</tr>
<tr>
<td>Hash Mask Length</td>
<td>Displays the hash mask length of the Bootstrap router.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Displays the time since the current E-BSR became the Bootstrap router.</td>
</tr>
</tbody>
</table>
### Sample Output

```bash
A:dut-d# show router pim status
===============================================================================
PIM Status
===============================================================================
Admin State : Up
Oper State : Up
BSR State : Accept Any
Elected BSR
  Address : None
  Expiry Time : N/A
  Priority : N/A
  Hash Mask Length : N/A
  Up Time : N/A
```

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPF Intf towards</td>
<td>Displays the RPF interface towards the elected BSR. The value is zero if there is no elected BSR in the network.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the address of the candidate BSR router.</td>
</tr>
<tr>
<td>Expiry Time</td>
<td>Displays the time remaining before the router sends the next Bootstrap message.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the priority of the Bootstrap router. The higher the value, the higher the priority.</td>
</tr>
<tr>
<td>Hash Mask Length</td>
<td>Displays the hash mask length of the candidate Bootstrap router.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Displays the time since becoming the Bootstrap router.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Displays the administrative status of CRP.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Displays the current operating state of the C-RP mechanism.</td>
</tr>
<tr>
<td>Address</td>
<td>Displays the local RP address.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the CRP's priority for becoming a rendezvous point (RP). A 0 value is the highest priority.</td>
</tr>
<tr>
<td>Holdtime</td>
<td>Displays the hold time of the candidate RP. It is used by the Bootstrap router to timeout the RP entries if it does not listen to another CRP advertisement within the holdtime period.</td>
</tr>
<tr>
<td>Policy</td>
<td>Displays the PIM policies for a particular PIM instance.</td>
</tr>
<tr>
<td>Default Group</td>
<td>Displays the default core group address.</td>
</tr>
<tr>
<td>RPF Table</td>
<td>Displays the route table used for RPF check.</td>
</tr>
<tr>
<td>MC-ECMP-Hashing</td>
<td>Displays if hash-based multicast balancing of traffic over ECMP links is enabled or disabled.</td>
</tr>
</tbody>
</table>
IGMP Commands

RPF Intf towards E-BSR : N/A

Candidate BSR
Admin State : Down
Oper State : Down
Address : None
Priority : 0
Hash Mask Length : 30

Candidate RP
Admin State : Down
Oper State : Down
Address : None
Priority : 192
Holdtime : 150

MC-ECMP-Hashing : Enabled
Policy : None
Default Group : 239.1.1.1

RPF Table : rttable-m
===============================================================================

mld

Syntax    mld
Context    show>router
Description This command displays MLD related information.

group

Syntax    group [grp-ipv6-address]
Context    show>router>mld
Description This command displays MLD group information.
Parameters  

Values       ipv6-address  x:x:x:x:x:x:x (eight 16-bit pieces)
             x:x:x:x:x:d.d.d.d
             x: [0..FFFF]H
             d: [0..255]D

Output  *A:SR7# show router mld group
MLD Groups
===============================================================================

Page 196  7450 ESS OS Routing Protocols Guide
No Matching Entries

*A:SR7#

*A:SR7# show router mld interface

MLD Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Adm</th>
<th>Oper</th>
<th>Cfg/Opr</th>
<th>Num</th>
<th>Groups</th>
<th>Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querier</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ver</td>
<td></td>
<td>Groups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host4_Srcv1_IPv6</td>
<td>Up</td>
<td>Up</td>
<td>2/2</td>
<td>0</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>FE80::216:4DFF:104D:4D5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host1</td>
<td>Up</td>
<td>Up</td>
<td>2/2</td>
<td>0</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>FE80::216:4DFF:104D:4D5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host2</td>
<td>Up</td>
<td>Up</td>
<td>2/2</td>
<td>0</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>FE80::216:4DFF:104D:4D5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host3_vlan1</td>
<td>Up</td>
<td>Up</td>
<td>2/2</td>
<td>0</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>FE80::216:4DFF:104D:4D5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host3_vlan2</td>
<td>Up</td>
<td>Up</td>
<td>2/2</td>
<td>0</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>FE80::216:4DFF:104D:4D5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host3_vlan3</td>
<td>Up</td>
<td>Up</td>
<td>2/2</td>
<td>0</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>FE80::216:4DFF:104D:4D5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host3_vlan4</td>
<td>Up</td>
<td>Up</td>
<td>2/2</td>
<td>0</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>FE80::216:4DFF:104D:4D5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host3_vlan5</td>
<td>Up</td>
<td>Up</td>
<td>2/2</td>
<td>0</td>
<td>none</td>
<td></td>
</tr>
<tr>
<td>FE80::216:4DFF:104D:4D5B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*A:SR7# show router mld ssm-translate

MLD SSM Tranlate Entries

No Matching Entries

*A:SR7#

*A:SR7# show router mld group

MLD Groups

(3FFE:100::2:100,FF05::1:1)
Up Time: 0d 00:00:31
Fwd List: Host1

(3FFE:100::2:100,FF05::1:2)
Up Time: 0d 00:00:31
Fwd List: Host1

(3FFE:100::2:100,FF05::1:3)
Up Time: 0d 00:00:31
Fwd List: Host1

(3FFE:100::2:100,FF05::1:4)
Up Time: 0d 00:00:31
Fwd List: Host1

(3FFE:100::2:100,FF05::1:5)

*A:SR7#
*A:SR7# show router mld group ff05::1:1

MLD Groups

(3FFE:100::2:100,FF05::1:1)
Up Time : 0d 00:00:40
Fwd List : Host1
(*,G)/(S,G) Entries : 1

*A:SR7#

*A:SR7# show router mld group ff05::1

MLD Groups

No Matching Entries

interface

Syntax  interface [ip-int-name | ip-address] [group] [grp-ipv6-address] [detail]

Context  show>router>mld

Description  This command displays MLD interface information.

Parameters  ip-int-name|ip-address — Specifies the IP interface name or interface address.

  group grp-ipv6-address — Specifies the IPv6 group address.

  Values  ipv6-address x:x:x:x:x:x:x (eight 16-bit pieces)
                      x:x:x:x:d.d.d
                      x: [0..FFFF]H
                      d: [0..255]D

detail — Displays detailed information.

Output  *A:SR7# show router mld interface Host1 detail

MLD Interface Host1

Interface : Host1
Admin Status : Up
Oper Status : Up
Querier : FE80::216:4DFF:FED4:4D5B
Querier Up Time : 0d 00:02:18
Querier Expiry Time : N/A
Time for next query: 0d 00:15:25
Admin/Oper version : 2/2
Num Groups : 6000
Policy : none
Max Groups Allowed : No Limit
Max Groups Till Now: 6000
Query Interval : 0
Query Resp Interval: 0
Last List Qry Interval : 0

MLD Group
### Multicast

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Last Reporter</th>
<th>Interface</th>
<th>Expires</th>
<th>Up Time</th>
<th>V1 Host Timer</th>
<th>Type</th>
<th>Mode</th>
<th>Compat Mode</th>
<th>Source</th>
<th>Expires</th>
<th>Type</th>
<th>Fwd/Blk</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF05::1:1</td>
<td>FE80::1</td>
<td>Host1</td>
<td>N/A</td>
<td>0d 00:00:10</td>
<td>include</td>
<td>dynamic</td>
<td></td>
<td>MLD Version 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3FFE:100::2:100</td>
<td>0d 00:34:07</td>
<td>dynamic</td>
<td>Fwd</td>
</tr>
<tr>
<td>FF05::1:2</td>
<td>FE80::1</td>
<td>Host1</td>
<td>N/A</td>
<td>0d 00:00:11</td>
<td>include</td>
<td>dynamic</td>
<td></td>
<td>MLD Version 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3FFE:100::2:100</td>
<td>0d 00:34:07</td>
<td>dynamic</td>
<td>Fwd</td>
</tr>
<tr>
<td>FF05::1:3</td>
<td>FE80::1</td>
<td>Host1</td>
<td>N/A</td>
<td>0d 00:00:11</td>
<td>include</td>
<td>dynamic</td>
<td></td>
<td>MLD Version 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3FFE:100::2:100</td>
<td>0d 00:34:07</td>
<td>dynamic</td>
<td>Fwd</td>
</tr>
<tr>
<td>FF05::1:4</td>
<td>FE80::1</td>
<td>Host1</td>
<td>N/A</td>
<td>0d 00:00:12</td>
<td>include</td>
<td>dynamic</td>
<td></td>
<td>MLD Version 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3FFE:100::2:100</td>
<td>0d 00:34:06</td>
<td>dynamic</td>
<td>Fwd</td>
</tr>
</tbody>
</table>
MLD Group

command

Group Address : FF05::1:5
Last Reporter : FE80::1
Interface     : Host1                   Expires       : N/A
Up Time       : 0d 00:00:12             Mode          : include
V1 Host Timer : Not running             Type          : dynamic
Compat Mode   : MLD Version 2

Source
Expires       Type    Fwd/Blk
3FFE:100::2:100 0d 00:34:06 dynamic Fwd

ssm-translate

Syntax ssm-translate
Context show>router>mld
Description This command displays the MLD SSM translate configuration.

static

Syntax static [ip-int-name | ip-address]
Context show>router>mld
Description This command displays MLD static group/source configuration.
Parameters ip-int-name|ip-address — iSpecifies the IP interface name or IP address.
Output
*A:SR7# show router mld static
MLD Static Group Source
Source                                  Group
Interface
No Matching Entries
*A:SR7#

*A:SR7# show router mld statistics
MLD Interface Statistics
Message Type    Received    Transmitted
Queries         0              640
Report V1       0              0
Report V2           10             0
Dones               0              0
-------------------------------------------------
General Interface Statistics
-------------------------------------------------
Bad Length        : 0
Bad Checksum      : 0
Unknown Type      : 0
Bad Receive If    : 0
Rx Non Local      : 0
Rx Wrong Version  : 0
Policy Drops      : 0
No Router Alert   : 0
Rx Bad Encodings  : 0
Rx Pkt Drops      : 0
Local Scope Pkts  : 10
Resvd Scope Pkts  : 0
-------------------------------------------------
Source Group Statistics
-------------------------------------------------
(S,G)             : 0
(*,G)             : 0
===============================================================================
MLD Status
===============================================================================
Admin State                       : Up
Oper State                        : Up
Query Interval                    : 1024
Last Listener Query Interval      : 1
Query Response Interval           : 10
Robust Count                      : 2
===============================================================================

statistics
Syntax        statistics [ip-int-name | ipv6-address]
Context       show>router>mld
Description   This command displays MLD statistics.
              ip-int-name|ipv6-address — iSpecifies the IP interface name or IPv6 address.

status
Syntax        status
Context       show>router>mld
Description   This command displays the MLD status.
Output        *A:SR7# show router mld status

MLD Status
===============================================================================
Admin State                       : Up
Oper State                        : Up
Query Interval                    : 1024
Last Listener Query Interval      : 1
Query Response Interval           : 10
Robust Count                      : 2
===============================================================================

group

**Syntax**  
`group [group-name] [detail]`

**Context**  
`show>router>msdp`

**Description**  
This command displays information about MSDP groups.

**Parameters**  
- `group-name` — Displays information about the specified group name. If no `group-name` is specified, information about all `group-name` displays.
- `detail` — Displays detailed MSDP group information.

**Output**  
**MSDP Group Output** — The following table provides MSDP group field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Displays the MSDP group name.</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the groups of peers in a full mesh topology to limit excessive flooding of source-active messages to neighboring peers.</td>
</tr>
<tr>
<td>Act Srcs</td>
<td>Displays the configured maximum number of active source messages that will be accepted by MSDP.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Displays the local end of a MSDP session.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Displays the administrative state.</td>
</tr>
<tr>
<td>Receive Msg Rate</td>
<td>Displays rate that the messages are read from the TCP session.</td>
</tr>
<tr>
<td>Receive Msg Time</td>
<td>Displays the time of MSDP messages that are read from the TCP session within the configured number of seconds.</td>
</tr>
<tr>
<td>Receive Msg Thd</td>
<td>Displays the configured threshold number of MSDP messages can be processed before the MSDP message rate limiting function.</td>
</tr>
<tr>
<td>SA Limit</td>
<td>Displays the source-active limit.</td>
</tr>
</tbody>
</table>
Sample Output

*A:ALA-48>show>router>msdp# group
MSDP Groups

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Mode</th>
<th>Act Srcs</th>
<th>Local Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>main</td>
<td>Mesh-group</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>loop1</td>
<td>Mesh-group</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>loop2</td>
<td>Mesh-group</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>loop3</td>
<td>Mesh-group</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>loop4</td>
<td>Mesh-group</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>loop5</td>
<td>Mesh-group</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

Groups : 6

*A:ALA-48>show>router>msdp#

*A:ALA-48>show>router>msdp# group test
MSDP Groups

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Mode</th>
<th>Act Srcs</th>
<th>Local Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>test</td>
<td>Mesh-group</td>
<td>50000</td>
<td>10.10.10.103</td>
</tr>
</tbody>
</table>

Groups : 1

*A:ALA-48>show>router>msdp#

*A:ALA-48>show>router>msdp# group test detail
MSDP Groups

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Local Address</th>
<th>Admin State</th>
<th>Receive Msg Rate</th>
<th>Receive Msg Thd</th>
<th>Mode</th>
<th>SA Limit</th>
<th>Export Policy</th>
<th>Import Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>test</td>
<td>10.10.10.103</td>
<td>Up</td>
<td>None</td>
<td>None</td>
<td>Mesh-group</td>
<td>50000</td>
<td>None Specified / Inherited</td>
<td>None Specified / Inherited</td>
</tr>
</tbody>
</table>

Groups : 1

*A:ALA-48>show>router>msdp#
peer

Syntax peer [ip-address] [group group-name] [detail]

Context show>router>msdp

Description This command displays information about an MSDP peer.

Parameters ip-address — Displays information about the specified IP address. If no IP address specified, information about all MSDP IP addresses display.

group group-name — Displays information about the specified group name. If no group-name is specified, information about all MSDP peers display.

detail — Displays detailed MSDP peer information.

Output MSDP Peer Output — The following table provides MSDP field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>Displays the IP address of the peer.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Displays the local IP address.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the current state of the peer.</td>
</tr>
<tr>
<td>Last State Change</td>
<td>Displays the date and time of the peer’s last state change.</td>
</tr>
<tr>
<td>SA Learnt</td>
<td>The number of SAs learned through a peer.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-48# show router msdp peer

MSDP Peers

<table>
<thead>
<tr>
<th>Peer</th>
<th>Local Address</th>
<th>State</th>
<th>Last State Change</th>
<th>SA Learnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.1.1</td>
<td>10.20.1.6</td>
<td>Established</td>
<td>08/30/2002 03:22:13</td>
<td>1008</td>
</tr>
</tbody>
</table>

Peers : 1

A:ALA-48#

A:ALA-48# show router msdp peer detail

MSDP Peers

<table>
<thead>
<tr>
<th>Peer Address</th>
<th>10.20.1.1</th>
</tr>
</thead>
</table>

Group Name : None
Local Address : 10.20.1.6
Last State Change : 08/30/2002 03:22:13 Last Act Src Limit : N/A
Peer Admin State : Up Default Peer : No
Peer Connect Retry : 0 State : Established
SA accepted        : 1008               SA received        : 709
State timer expires: 18                 Peer time out      : 62
Active Source Limit: None               Receive Msg Rate : 0
Receive Msg Time   : 0                  Receive Msg Thd : 0
Auth Status        : Disabled           Auth Key           : None
Export Policy      : None Specified / Inherited
Import Policy      : None Specified / Inherited
-------------------------------------------------------------------------------
Peers : 1
-------------------------------------------------------------------------------
A:ALA-48#

source

Syntax source [ip-address/mask] [type {configured | dynamic | both}] [detail]

Context show>router>msdp

Description This command displays the discovery method for this multicast source.

Parameters configured — Displays user-created sources.
dynamic — Displays dynamically created sources.
both — Displays both user-configured and dynamically created sources.
detail — Displays detailed MSDP source information.

Output MSDP Source Output — The following table provides MSDP source field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Displays the IP address of the peer.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of peer.</td>
</tr>
<tr>
<td>SA limit</td>
<td>Displays the local IP address.</td>
</tr>
<tr>
<td>State</td>
<td>Displays the current state of the peer.</td>
</tr>
<tr>
<td>Num excd</td>
<td>Indicates the number of times the global active source limit has been exceeded.</td>
</tr>
<tr>
<td>Last exceeded</td>
<td>Displays the date and time of the peer’s last state change.</td>
</tr>
</tbody>
</table>

source-active

Syntax source-active [group ip-address | local | originator ip-address | peer ip-address | source ip-address ] [group ip-address source ip-address] [detail]

Context show>router>msdp

Description This command displays source active messages accepted by MSDP.
Parameters

- **group ip-address** — Displays information about the specified group IP address.
- **local** — Displays information about local source-active messages.
- **originator ip-address** — Displays information about the specified originator IP address.
- **peer ip-address** — Displays information about the specified peer IP address.
- **source ip-address** — Displays information about the specified source IP address.
- **group ip-address** — Displays information about the specified group IP address.

**detail** Displays detailed MSDP source-active information.

Output

**MSDP Source-Active Output** — The following table provides MSDP source-active field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grp Address</td>
<td>Displays the IP address of the group.</td>
</tr>
<tr>
<td>Src Address</td>
<td>Displays the IP address of the source.</td>
</tr>
<tr>
<td>Origin RP</td>
<td>Displays the origination rendezvous point (RP) address.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>Displays the address of the peer.</td>
</tr>
<tr>
<td>State Timer</td>
<td>The time-out value. If the value reaches zero, the SA is removed.</td>
</tr>
</tbody>
</table>

Sample Output

```
A:ALA-48# show router msdp source-active
MSDP Source Active Info
Grp Address      Src Address      Origin RP        Peer Address State Timer
-------------------------------------------------------------------------------
228.100.0.0      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.1      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.2      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.3      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.4      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.5      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.6      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.7      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.8      100.112.1.2      10.20.1.1        10.20.1.1 69
228.100.0.9      100.112.1.2      10.20.1.1        10.20.1.1 69
-------------------------------------------------------------------------------
MSDP Source Active : 10
A:ALA-48# show router msdp source-active detail
MSDP Source Active
Group Address : 228.100.0.0  Source Address : 100.112.1.2
Origin RP     : 10.20.1.1    Peer Address    : 10.20.1.1
State Timer   : 64          Up Time        : 3d 01:44:25
```
source-active-rejected

Syntax **source-active-rejected** [peer-group *name*] [group *ip-address*] [source *ip-address*] [originator *ip-address*] [peer *ip-address*]

Context `show>router>msdp`

Description This command displays source active messages rejected by MSDP.

Parameters **group *ip-address*** — Displays information about the peer group name of the Source Active entry that is rejected.

**local** — Displays information about local source-active messages.

**originator *ip-address*** — Displays information about the specified originator IP address.

**peer *ip-address*** — Displays information about the peer from which this rejected source active entry was last received.

**source *ip-address*** — Displays information about the source address of the source active entry that is rejected.

**group *ip-address*** — Displays information about the specified group IP address.
**MSDP Source-Active Output** — The following table provides MSDP source-active field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grp Address</td>
<td>Displays the IP address of the group.</td>
</tr>
<tr>
<td>Src Address</td>
<td>Displays the IP address of the source.</td>
</tr>
<tr>
<td>Origin RP</td>
<td>Displays the origination rendezvous point (RP) address.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>Displays the address of the peer.</td>
</tr>
<tr>
<td>Reject Reason</td>
<td>Displays the reason why this source active entry is rejected.</td>
</tr>
</tbody>
</table>

**Sample Output**

* A:ALA-48# show router msdp source-active-rejected

<table>
<thead>
<tr>
<th>Grp Address</th>
<th>Src Address</th>
<th>Origin RP</th>
<th>Peer Address</th>
<th>Reject Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>228.100.0.1</td>
<td>110.0.0.1</td>
<td>10.20.0.1</td>
<td>20.0.0.1</td>
<td>Import Policy</td>
</tr>
<tr>
<td>228.100.0.2</td>
<td>110.0.0.2</td>
<td>10.20.0.2</td>
<td>20.0.0.2</td>
<td>Export Policy</td>
</tr>
<tr>
<td>228.100.0.3</td>
<td>110.0.0.3</td>
<td>10.20.0.3</td>
<td>20.0.0.3</td>
<td>RPF Failure</td>
</tr>
<tr>
<td>228.100.0.4</td>
<td>110.0.0.4</td>
<td>10.20.0.4</td>
<td>20.0.0.4</td>
<td>Limit Exceeded</td>
</tr>
<tr>
<td>228.100.0.5</td>
<td>110.0.0.5</td>
<td>10.20.0.5</td>
<td>20.0.0.5</td>
<td>Limit Exceeded</td>
</tr>
<tr>
<td>228.100.0.6</td>
<td>110.0.0.6</td>
<td>10.20.0.6</td>
<td>20.0.0.6</td>
<td>Limit Exceeded</td>
</tr>
<tr>
<td>228.100.0.7</td>
<td>110.0.0.7</td>
<td>10.20.0.7</td>
<td>20.0.0.7</td>
<td>Limit Exceeded</td>
</tr>
</tbody>
</table>

SA Rejected Entries : 7

*A:ALA-48#

**statistics**

**Syntax**

`statistics [peer ip-address]`

**Context**

`show>router>msdp`

**Description**

This command displays statistics information related to a MSDP peer.

**Parameters**

`peer ip-address` — Displays information about the specified peer IP address

**Output**

**MSDP Statistics Output** — The following table provides MSDP statistics field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last State Change</td>
<td>Displays the date and time the peer state changed.</td>
</tr>
<tr>
<td>RPF Failures</td>
<td>Displays the number of reverse path forwarding (RPF) failures.</td>
</tr>
<tr>
<td>SA Msgs Sent</td>
<td>Displays the number of source-active messages sent.</td>
</tr>
</tbody>
</table>
Sample Output

A:ALA-48# show router msdp statistics
MSDP Statistics
Glo ActSrc Lim Excd: 0
Peer Address : 10.20.1.1
Last State Change : 0d 11:33:16  Last message Peer : 0d 00:00:17
RPF Failures : 0  Remote Closes : 0
SA Msgs Sent : 0  SA Msgs Recvd : 709
SA req. Msgs Sent : 0  SA req. Msgs Recvd : 0
SA res. Msgs Sent : 0  SA res. Msgs Recvd : 0
KeepAlive Msgs Sent : 694  KeepAlive Msgs Recvd: 694
Unknown Msgs Sent : 0  Error Msgs Recvd : 0
Peers : 1

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA req. Msgs Sent</td>
<td>Displays the number of source-active request messages sent.</td>
</tr>
<tr>
<td>SA res. Msgs Sent</td>
<td>Displays the number of source-active response messages sent.</td>
</tr>
<tr>
<td>KeepAlive Msgs Sent</td>
<td>Displays the number of keepalive messages sent.</td>
</tr>
<tr>
<td>Unknown Msgs Sent</td>
<td>Displays the number of unknown messages received.</td>
</tr>
<tr>
<td>Last message Peer</td>
<td>Displays the time the last message was received from the peer.</td>
</tr>
<tr>
<td>Remote Closes</td>
<td>Displays the number of times the remote peer close.</td>
</tr>
<tr>
<td>SA Msgs Recvd</td>
<td>Displays the number of source-active messages received.</td>
</tr>
<tr>
<td>SA req. Msgs Recvd</td>
<td>Displays the number of source-active request messages received.</td>
</tr>
<tr>
<td>SA res. Msgs Recvd</td>
<td>Displays the number of source-active response messages received.</td>
</tr>
<tr>
<td>KeepAlive Msgs Recd</td>
<td>Displays the number of keepalive messages received.</td>
</tr>
<tr>
<td>Error Msgs Recvd</td>
<td>Displays the number of unknown messages received.</td>
</tr>
</tbody>
</table>
status

Syntax status

Context show>router>msdp

Description This command displays MSDP status information.

Output MSDP Status Output — The following table provides MSDP status field descriptions.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin State</td>
<td>Displays the administrative state.</td>
</tr>
<tr>
<td>Local Address</td>
<td>Displays the local IP address.</td>
</tr>
<tr>
<td>Active Src Limit</td>
<td>Displays the active source limit.</td>
</tr>
<tr>
<td>Act Src Lim Excd</td>
<td>Displays the active source limit which has been exceeded.</td>
</tr>
<tr>
<td>Num. Peers</td>
<td>Displays the number of peers.</td>
</tr>
<tr>
<td>Num. Peers Estab</td>
<td>Displays the number of peers established.</td>
</tr>
<tr>
<td>Num. Source Active</td>
<td>Displays the number of active sources.</td>
</tr>
<tr>
<td>Policies</td>
<td>The policy to export source active state from the source active list into MSDP.</td>
</tr>
<tr>
<td>Data Encapsulation</td>
<td>The rendezvous point (RP) using MSDP to encapsulate multicast data received in MSDP register messages inside forwarded MSDP source-active messages - enabled or disabled.</td>
</tr>
<tr>
<td>Rate</td>
<td>The receive message rate.</td>
</tr>
<tr>
<td>Time</td>
<td>The receive message time.</td>
</tr>
<tr>
<td>Threshold</td>
<td>The number of MSDP messages that can be processed before the MSDP message rate limiting function is activated.</td>
</tr>
<tr>
<td>RPF Table</td>
<td>The name of the reverse path forwarding table.</td>
</tr>
<tr>
<td>Last mdsp Enabled</td>
<td>The time the last MDSP was triggered.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-48# show router msdp status
===============================================================================
MSDP Status
===============================================================================
Admin State : Up
Local Address : None
Global Statistics
Active Src Limit : None
mcac

Syntax mcac

Context show>router

Description This command enables the context to display multicast CAC related information.

policy

Syntax policy policy-name [bundle bundle-name] [protocol protocol-name] [interface if-name] [detail]

Context show>router>mcac

Description This command displays MCAC policy information.

Parameters policy-name — Specifies an existing multicast CAC (MCAC) policy name.

bundle bundle-id — Specifies an existing multicast bundle name.

protocol protocol-name — specifies an applicable protocol to display.

Values igmp, pim, igmpSnpg

interface if-name — Specifies an interface name to display.

detail — Displays detailed information.

Sample Output

*A:ALA-48>show>router>mcac# policy

===============================================================================
Multicast CAC Policies
===============================================================================
<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>btv_fr</td>
<td>foreign TV offering</td>
</tr>
<tr>
<td>btv_vl</td>
<td>eastern TV offering</td>
</tr>
<tr>
<td>policy1</td>
<td>this is policy1</td>
</tr>
</tbody>
</table>
IGMP Commands

policy2
this is policy 2

Policies : 4

*A:ALA-48>show>router>mcac#

*A:ALA-48>show>router>mcac# policy btv_fr

Multicast CAC policy

Policy : btv_fr
Description : foreign TV offering
Default Action : discard
Bundle(s) : FOR

*A:ALA-48>show>router>mcac#

statistics

Syntax statistics policy policy-name [bundle bundle-name] [protocol protocol-name] [interface if-name] statistics

Context show>router>mcac

Description This command displays MCAC statistics.

Parameters policy-name — Specifies an existing multicast CAC (MCAC) policy name.
bundle bundle-id — Displays statistics for the specified existing multicast bundle name.
protocol protocol-name — Displays statistics for the specified applicable protocol.

Values igmp, pim, igmpSnpg

interface if-name — Displays statistics for the specified interface name.
detail — Displays detailed information.

mvpn

Syntax mvpn

Context show>router router-instance

Description This command displays Multicast VPN related information. The router instance must be specified.

Sample Output

*A:Dut-C# show router 1 mvpn

MVPN 1 configuration data

Page 212 7450 ESS OS Routing Protocols Guide
signaling : Bgp  auto-discovery : Enabled
UMH Selection : Highest-Ip intersite-shared : Enabled
vrf-import : N/A
vrf-export : N/A
vrf-target : target:1:1
C-Mcast Import RT : target:10.20.1.32
ipmsi : pim-asm 224.1.1.1
admin status : Up  three-way-hello : N/A
hello-interval : N/A  hello-multiplier : 35 * 0.1
tracking support : Disabled  Improved Assert : N/A
spmsi : pim-ssm 225.0.0.0/32
join-tlv-packing : N/A
data-delay-interval : 3 seconds
data-threshold : 224.0.0.0/4 --> 1 kbps

---

tunnel-table

**Syntax**

tunnel-table [ip-address [mask]] [protocol | sdp sdp-id]
tunnel-table [summary]

**Context**

show>router

**Description**

This command displays tunnel table information.

**Parameters**

`protocol` — Specifies the protocol.

Values: bgp | ldp | rsvp | sdp

`sdp-id` — Specifies the SDP ID.

Values: 1..17407

**Output**

```
*A:Dut-C# show router tunnel-table sdp 17407

Tunnel Table (Router: Base)

+-----------------+-----------------+-----------------+-----------------+-----------------+
| Destination     | Owner Encap TunnelId Pref Nexthop  Metric |
|-----------------|-----------------+-----------------+-----------------+-----------------|
| 127.0.68.0/32   | sdp             | MPLS            | 17407           | 5               |
| 127.0.68.0      |                 |                 |                 | 127.0.68.0      | 0               |
```
Clear Commands

database

Syntax:
- `database [interface ip-int-name|ip-address] [group grp-ip-address [source src-ip-address]]`
- `database grp-interface interface-name [fwd-service service-id]`
- `database [interface ip-int-name|ip-address] [group grp-ip-address source src-ip-address]`
- `database host [ip-address]`
- `database interface ip-int-name|ip-address [group grp-ip-address] [source src-ip-address]`

Context: `clear>router>igmp`

Description: This command clears IGMP or PIM database statistics on a specified interface or IP address.

Parameters:
- `interface ip-int-name` — Clears the IGMP or PIM database on the specified interface.
- `interface ip-address` — Clears the IGMP or PIM database on the specified IP address.
- `group group-ip-address` — Clears the multicast group address(ipv4/ipv6) or zero in the specified address group.
- `source ip-address` — Clears the IGMP or PIM database from the specified source IP address.
- `family` — Clears either IPv4 or IPv6 information.
- `mpls-if-name` — Clears the MPLS interface name.
Syntax: \texttt{mpls-if-index}

\textbf{statistics}

\textbf{Syntax} \texttt{statistics [interface ip-int-name | ip-address]}

\textbf{Context} \texttt{clear>router>igmp}

\textbf{Description} This command clears IGMP statistics on a specified interface or IP address. Note that interface and group/source cannot be specified at the same time.

\textbf{Parameters}

- \texttt{interface ip-int-name} — Clears IGMP statistics on the specified interface.
- \texttt{interface ip-address} — Clears IGMP statistics on the specified IP address.
- \texttt{interface mt-int-name} — Clears the default core group address of the Multicast Distribution Tree (MDT) for the VPRN instance. The Multicast Tunnel (MT) interface for a VPRN is created when this object is set to a valid group address.

\textbf{Syntax}: \texttt{vprn-id-mt-grp-ip-address}

\textbf{s-pmsi}

\textbf{Syntax} \texttt{s-pmsi [mdSrcAddr] [mdGrpAddr] [vprnSrcAddr vprnGrpAddr]}

\textbf{Context} \texttt{clear>router>pim}

\textbf{Description} This command clears PIM selective provider multicast service interface cache.

\textbf{Parameters}

- \texttt{mdSrcAddr} — Clears the specified source address used for Multicast Distribution Tree (MDT).
- \texttt{mdGrpAddr} — Clears the specified group address used for Multicast Distribution Tree (MDT).
- \texttt{vprnSrcAddr} — Clears the specified source address of the multicast sender.
- \texttt{vprnGrpAddr} — Clears the specified multicast group address.

\textbf{statistics}

\textbf{Syntax} \texttt{statistics [[interface ip-int-name | ip-address | mt-int-name]] [group grp-ip-address [source ip-address]] [family]]}

\textbf{Context} \texttt{clear>router>pim}

\textbf{Description} This command clears PIM statistics on a specified interface or IP address. Note that an interface and group or source cannot be specified at the same time.

\textbf{Parameters}

- \texttt{interface ip-int-name} — Clears PIM statistics on the specified interface.
- \texttt{interface ip-address} — Clears PIM statistics on the specified IP address.
interface mt-int-name — Clears the default core group address of the Multicast Distribution Tree (MDT) for the VPRN instance. The Multicast Tunnel (MT) interface for a VPRN is created when this object is set to a valid group address.

**syntax:** vprn-id-mt-grp-ip-address

**group grp-ip-address** — When only the group address is specified and no source is specified, (*,G) statistics are cleared. When the group address is specified along with the source address, then the (S,G) statistics are reset to zero.

**source ip-address** — When the source address is specified along with the group address, then the (S,G) statistics are reset to zero.

**family** — Clears either IPv4 or IPv6 information.

### Version

**Syntax**

```
version [interface ip-int-name | ip-address]
```

**Context**
clear>router>igmp

**Description**
This command clears IGMP statistics on a specified interface or IP address.

**Parameters**

- **interface ip-int-name** — Clears IGMP or PIM statistics on the specified interface.
- **interface ip-address** — Clears IGMP or PIM statistics on the specified IP address.

### MLD

**Syntax**

```
mld
```

**Context**
clear>router

**Description**
This command enables the context to to clear and reset Multicast Listener Discovery (MLD) entities.

### Database

**Syntax**

```
database [interface ip-int-name|ipv6-address] [group ip-address [source ip-address]]
```

**Context**
clear>router>mld

**Description**
This command clears Multicast Listener Discovery (MLD) database parameters.

**Parameters**

- **interface ip-int-name** — Clears database information for the specified Multicast Listener Discovery (MLD) interface name.
- **interface ipv6-address** — Clears database information for the specified Multicast Listener Discovery (MLD) interface IPv6 address.
group ip-address — Clears database information for the specified Multicast Listener Discovery (MLD) group IP address.

source ip-address — Clears database information for the specified Multicast Listener Discovery (MLD) source IP address.

### statistics

**Syntax**

```
statistics [ip-int-name|ipv6-address]
```

**Context**

```
clear>router>mld
```

**Description**

This command clears Multicast Listener Discovery (MLD) statistics parameters.

**Parameters**

- `ip-int-name` — Clears statistics for the specified Multicast Listener Discovery (MLD) interface name.
- `ipv6-address` — Clears statistics for the specified Multicast Listener Discovery (MLD) IPv6 address.

### version

**Syntax**

```
version [ip-int-name|ip-address]
```

**Context**

```
clear>router>mld
```

**Description**

This command clears Multicast Listener Discovery (MLD) version parameters.

**Parameters**

- `ip-int-name` — Clears version information for the specified Multicast Listener Discovery (MLD) interface name.
- `ip-address` — Clears version information for the specified Multicast Listener Discovery (MLD) IP address.

### msdp

**Syntax**

```
msdp
```

**Context**

```
clear>router
```

**Description**

This command enables the context to clear and reset Multicast Source Discovery protocol (MSDP) entities and statistics.

### cache

**Syntax**

```
cache [peer ip-address] [group ip-address] [source ip-address] [originrp ip-address]
```

**Context**

```
clear>router>msdp
```

**Description**

This command clears the MSDP cache.
IGMP Commands

Parameters

**peer ip-address** — Clears the cache of the IP address of the peer to which Multicast Source Discovery protocol (MSDP) source-active (SA) requests for groups matching this entry's group range were sent.

**group ip-address** — Clears the group IP address of the SA entry.

**source ip-address** — Clears the source IP address of the SA entry.

**originrp ip-address** — Clears the origin rendezvous point (RP) address type of the SA entry.

Statistics

**Syntax**

```
statistics [peer ip-address]
```

**Context**

```
clear>router>msdp
```

**Description**

**peer ip-address** — Clears the statistics of the IP address of the peer to which Multicast Source Discovery Protocol (MSDP) source-active (SA) requests for groups matching this entry's group range were sent.

Neighbor

**Syntax**

```
neighbor [ip-int-name | ip-address] [family]
```

**Context**

```
clear>router>pim
```

**Description**

This command clears PIM neighbor data on a specified interface or IP address.

**Parameters**

**ip-int-name** — Clears PIM neighbor on the specified interface.

**ip-address** — Clears PIM neighbor on the specified IP address.

**family** — Clears either IPv4 or IPv6 information.

IGMP Snooping

**Syntax**

```
igmp-snooping
```

**Context**

```
clear>service>id
```

**Description**

This command enables the context to clear IGMP snooping-related data.

Port-DB

**Syntax**

```
port-db [sap sap-id | sdp sdp-id:vc-id] [group grp-address [source ip-address]]
```

**Context**

```
clear>service>id>igmp-snooping
```

**Description**

Clears the information on the IGMP snooping port database.
**Parameters**  

<table>
<thead>
<tr>
<th>sap sap-id</th>
<th>Clears IGMP snooping statistics matching the specified SAP ID and optional encapsulation value. The sap-id can be in one of the following formats:</th>
</tr>
</thead>
</table>
| **.sap-id** | **Syntax**  
| sap-id | **Example**  

<table>
<thead>
<tr>
<th>Encapsulation type</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>port-id</td>
<td>1/1/3</td>
</tr>
<tr>
<td>dot1q</td>
<td>port-id :qtag1</td>
<td>1/1/3:100</td>
</tr>
<tr>
<td>qinq</td>
<td>port-id :qtag1.qtag2</td>
<td>1/1/3:100.200</td>
</tr>
</tbody>
</table>

qtag1, qtag2 — The encapsulation value on the specified port ID.  

| Values | 0 — 4094 |

<table>
<thead>
<tr>
<th>sdp sdp-id</th>
<th>Clears only IGMP snooping entries associated with the specified mesh SDP or spoke SDP. For a spoke SDP, the VC ID must be specified; for a mesh SDP, the VC ID is optional.</th>
</tr>
</thead>
</table>
| **sdp-id** | **Values**  
| 1 — 17407 |

vc-id — The virtual circuit ID on the SDP ID for which to clear information.  

| Default | For mesh SDPs only, all VC IDs |
| Values | 1 — 4294967295 |

<table>
<thead>
<tr>
<th>group grp-address</th>
<th>Clears IGMP snooping statistics matching the specified group address.</th>
</tr>
</thead>
</table>

| source ip-address | Clears IGMP snooping statistics matching one particular source within the multicast group. |

**querier**  

<table>
<thead>
<tr>
<th>Syntax</th>
<th>querier</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Context</strong></td>
<td>clear&gt;service&gt;id&gt;igmp-snooping</td>
</tr>
</tbody>
</table>

| Description | Clears information on the IGMP snooping queriers for the VPLS service. |

**statistics**  

| Syntax | statistics [sap sap-id | sdp sdp-id:vc-id] |
|--------|-----------------------------|
| **Context** | clear>service>id>igmp-snooping |

| Description | Clears IGMP snooping statistics for the VPLS service. |

| Parameters | sap sap-id | Displays IGMP snooping statistics for a specific SAP. The sap-id can be in one of the following formats:  
|------------|-----------------------------------|
| sap-id | **Syntax**  
| sap-id | **Example**  

<table>
<thead>
<tr>
<th>Encapsulation type</th>
<th>Syntax</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>null</td>
<td>port-id</td>
<td>1/1/3</td>
</tr>
<tr>
<td>dot1q</td>
<td>port-id :qtag1</td>
<td>1/1/3:100</td>
</tr>
<tr>
<td>qinq</td>
<td>port-id :qtag1.qtag2</td>
<td>1/1/3:100.200</td>
</tr>
</tbody>
</table>
IGMP Commands

qtag1, qtag2 — The encapsulation value on the specified port ID.

Values  
0 — 4094

sdp sdp-id — Displays the IGMP snooping statistics for a specific spoke or mesh SDP.

Values  
1 — 17407

vc-id — The virtual circuit ID on the SDP ID for which to display information.

Default  
For mesh SDPs only, all VC IDs

Values  
1 — 4294967295

pim-snooping

Syntax  
pim-snooping

Context  
clear>service>id

Description  
This command enables the context to clear PIM snooping information.

database

Syntax  
database [[sap sap-id] | sdp sdp-id:vc-id] [group grp-ip-address] [source src-ip-address]]

Context  
clear>service>id>pim-snooping

Description  
This command clears PIM snooping source group database information.

Parameters  
sap sap-id — Clears PIM snooping SAP information.

sdp sdp-id — Clears PIM snooping entries associated with the specified SDP. For a spoke SDP, the VC ID must be specified; for a mesh SDP, the VC ID is optional.

Values  
1 — 17407

group grp-address — Clears PIM snooping information matching the specified group address.

source ip-address — Clears PIM snooping information matching one particular source within the multicast group.

neighbor

Syntax  
neighbor [ip-address | sap sap-id | sdp sdp-id:vc-id]

Context  
clear>service>id>pim-snooping

Description  
This command clears PIM snooping neighbor information.

Parameters  
ip-address — Clears IP address information.
**Statistics**

**Syntax**

```
statistics [sap sap-id | sdp sdp-id:vc-id]
```

**Context**

clear>service>id>pim-snooping

**Description**

This command clears PIM snooping statistics for the specified SAP or SDP.

**Parameters**

- **sap sap-id** — Clears PIM snooping SAP information.
- **sdp sdp-id** — Clears PIM snooping entries associated with the specified SDP. For a spoke SDP, the VC ID must be specified; for a mesh SDP, the VC ID is optional.

**Values**

1 — 17407
Debug Commands

Debug IGMP Commands

group-interface

Syntax [no] group-interface [fwd-service service-id] [ip-int-name]
Context debug>router>igmp
Description This command enables debugging for IGMP group-interface.
The no form of the command disables debugging.

host

Syntax host [ip-address]
host [fwd-service service-id] group-interface ip-int-name
no host [ip-address]
no host [fwd-service service-id] group-interface ip-int-name
Context debug>router>igmp
Description This command enables debugging for the IGMP host.
The no form of the command disables debugging.

interface

Syntax [no] interface [ip-int-name | ip-address]
Context debug>router>igmp
Description This command enables debugging for IGMP interfaces.
The no form of the command disables the IGMP interface debugging for the specifies interface name or IP address.
Parameters
ip-int-name — Only displays the information associated with the specified IP interface name.
ip-address — Only displays the information associated with the specified IP address.
### Multicast

#### mcs

**Syntax**

```
mcs [ip-int-name]
no mcs
```

**Context**
debug>router>igmp

**Description**
This command enables debugging for IGMP multicast servers (MCS).

The `no` form of the command disables the IGMP interface debugging for the specified interface name.

**Parameters**
- `ip-int-name` — Only displays the information associated with the specified IP interface name.

#### misc

**Syntax**

```
[no] misc
```

**Context**
debug>router>igmp

**Description**
This command enables debugging for IGMP miscellaneous.

The `no` form of the command disables the debugging.

**Sample Output**

```
A:ALA-CA# debug router 100 igmp misc
*A:ALA-CA# show debug
debug
  router "100"
    igmp
      misc
      exit
  exit
  exit
*A:ALA-CA#
```

#### packet

**Syntax**

```
packet [query|v1-report|v2-report|v3-report|v2-leave] host ip-address
no packet [query|v1-report|v2-report|v3-report|v2-leave] [ip-int-name|ip-address]
```

**Context**
debug>router>igmp

**Description**
This command enables/disables debugging for IGMP packets.

**Parameters**
- `query` — Specifies to log the IGMP group- and source-specific queries transmitted and received on this interface.
- `v1-report` — Specifies to log IGMP V1 reports transmitted and received on this interface.
**v2-report** — Specifies to log IGMP V2 reports transmitted and received on this interface.

**v3-report** — Specifies to log IGMP V3 reports transmitted and received on this interface.

**v2-leave** — Specifies to log the IGMP Leaves transmitted and received on this interface.

**ip-int-name** — Only displays the information associated with the specified IP interface name.

**ip-address** — Only displays the information associated with the specified IP address.
Debug PIM Commands

adjacency

Syntax  [no] adjacency
Context  debug>router>pim
Description  This command enables/disables debugging for PIM adjacencies.

all

Syntax  all [group grp-ip-address] [source ip-address] [detail]
       no all
Context  debug>router>pim
Description  This command enables/disables debugging for all the PIM modules.
Parameters  group grp-ip-address — Debugs information associated with all PIM modules.
            Values  IPv4 or IPv6 address
            source ip-address — Debugs information associated with all PIM modules.
            Values  IPv4 or IPv6 address
detail — Debugs detailed information on all PIM modules.

assert

Syntax  assert [group grp-ip-address] [source ip-address] [detail]
        no assert
Context  debug>router>pim
Description  This command enables/disables debugging for PIM assert mechanism.
Parameters  group grp-ip-address — Debugs information associated with the PIM assert mechanism.
            Values  multicast group address (ipv4/ipv6)
            source ip-address — Debugs information associated with the PIM assert mechanism.
            Values  source address (ipv4/ipv6)
detail — Debugs detailed information on the PIM assert mechanism.
bsr

Syntax  
bsr [detail]  
no bsr

Context  
debug>router>pim

Description  
This command enables debugging for PIM Bootstrap mechanism.  
The no form of the command disables debugging.

Parameters  
detail — Debugs detailed information on the PIM assert mechanism.

data

Syntax  
data [group grp-ip-address] [source ip-address] [detail]  
no data

Context  
debug>router>pim

Description  
This command enables/disables debugging for PIM data exception.

Parameters  
group grp-ip-address — Debugs information associated with the specified data exception.  
Values  
multicast group address (ipv4/ipv6)

source ip-address — Debugs information associated with the specified data exception.  
Values  
source address (ipv4/ipv6)

detail — Debugs detailed IP data exception information.

db

Syntax  
db [group grp-ip-address] [source ip-address] [detail]  
no db

Context  
debug>router>pim

Description  
This command enables/disables debugging for PIM database.

Parameters  
group grp-ip-address — Debugs information associated with the specified database.  
Values  
multicast group address (ipv4/ipv6) or zero

source ip-address — Debugs information associated with the specified database.  
Values  
source address (ipv4/ipv6)

detail — Debugs detailed IP database information.
interface

Syntax  interface [ip-int-name | mt-int-name | ip-address] [detail]
        no interface

Context  debug>router>pim

Description  This command enables/disables debugging for PIM interface.

Parameters  ip-int-name — Debugs the information associated with the specified IP interface name.

    Values  IPv4 or IPv6 interface address

    mt-int-address — Debugs the information associated with the specified VPRN ID and group address.

    ip-address — Debugs the information associated with the specified IP address.

    detail — Debugs detailed IP interface information.

jp

Syntax  jp [group grp-ip-address] [source ip-address] [detail]
        no jp

Context  debug>router>pim

Description  This command enables/disables debugging for PIM Join-Prune mechanism.

Parameters  group  grp-ip-address — Debugs information associated with the specified Join-Prune mechanism.

    Values  multicast group address (ipv4/ipv6) or zero

    source  ip-address — Debugs information associated with the specified Join-Prune mechanism.

    Values  source address (ipv4/ipv6)

    detail — Debugs detailed Join-Prune mechanism information.

mrib

Syntax  mrib [group grp-ip-address] [source ip-address] [detail]
        no mrib

Context  debug>router>pim

Description  This command enables/disables debugging for PIM MRIB.

Parameters  group  grp-ip-address — Debugs information associated with the specified PIM MRIB.

    Values  multicast group address (ipv4/ipv6)

    source  ip-address — Debugs information associated with the specified PIM MRIB.

    Values  source address (ipv4/ipv6)
Debug PIM Commands

**msg**

**Syntax**
```
msg [detail]
no msg
```

**Context**
debug>router>pim

**Description**
This command enables/disables debugging for PIM messaging.

**Parameters**
detail — Debugs detailed messaging information.

**packet**

**Syntax**
```
packet [hello | register | register-stop | jp | bsr | assert | crp] [ip-int-name | ip-address]
no packet
```

**Context**
debug>router>pim

**Description**
This command enables/disables debugging for PIM packets.

**Parameters**
hello | register | register-stop | jp | bsr | assert | crp — PIM packet types.

*ip-int-name* — Debugs the information associated with the specified IP interface name.

**Values**
IPv4 or IPv6 interface address

*ip-address* — Debugs the information associated with the specified IP address of a particular packet type.

**register**

**Syntax**
```
register [group grp-ip-address] [source ip-address] [detail]
no register
```

**Context**
debug>router>pim

**Description**
This command enables/disables debugging for PIM Register mechanism.

**Parameters**
group grp-ip-address — Debugs information associated with the specified PIM register.

**Values**
multicast group address (ipv4/ipv6)

source ip-address — Debugs information associated with the specified PIM register.

**Values**
source address (ipv4/ipv6)

detail — Debugs detailed register information.
rtm
Syntax  
rtm [detail]
no rtm
Context  
debug>router>pim
Description  
This command enables/disables debugging for PIM RTM.
Parameters  
detail — Debugs detailed RTM information.

s-pmsi
Syntax  
s-pmsi [{vpnSrcAddr [vpnGrpAddr]} [mdSrcAddr]] [detail]
no s-pmsi
Context  
debug>router>pim
Description  
This command enables debugging for PIM selective provider multicast service interface. The no form of the command disables the debugging.
Parameters  
vpnSrcAddr — Specifies the VPN source address.
vpnGrpAddr — Specifies the VPN group address
mdSrcAddr — Specifies the source address of the multicast sender.
detail — Displays detailed information for selective PMSI.

msdp
Syntax  
[no] msdp
Context  
debug>router
Description  
This command enables debugging for Multicast Source Discovery Protocol (MSDP). The no form of the command disables MSDP debugging.

packet
Syntax  
packet [pkt-type] [peer ip-address]
Context  
debug>router>msdp
Description  
This command enables debugging for Multicast Source Discovery Protocol (MSDP) packets. The no form of the command disables MSDP packet debugging.
Debug PIM Commands

Parameters

**pkt-type** — Debrids information associated with the specified packet type.

**Values**

keep-alive, source-active, sa-request, sa-response

**peer ip-address** — Debrids information associated with the specified peer IP address.

**pim**

**Syntax**

```
pim [grp-address]
no pim
```

**Context**

debug>router>msdp

**Description**

This command enables debugging for Multicast Source Discovery Protocol (MSDP) PIM.

The **no** form of the command disables MSDP PIM debugging.

**Parameters**

**grp-address** — Debrids the IP multicast group address for which this entry contains information.

**rtm**

**Syntax**

```
rtm [rp-address]
no rtm
```

**Context**

debug>router>msdp

**Description**

This command enables debugging for Multicast Source Discovery Protocol (MSDP) route table manager (RTM).

The **no** form of the command disables MSDP RTM debugging.

**Parameters**

**rp-address** — Debrids the IP multicast address for which this entry contains information.

**sa-db**

**Syntax**

```
sa-db [group grpAddr] [source srcAddr] [rp rpAddr]
no sadb
```

**Context**

debug>router>msdp

**Description**

This command enables debugging for Multicast Source Discovery Protocol (MSDP) source-active requests.

The **no** form of the command disables the MSDP source-active database debugging.

**Parameters**

**group grpAddr** — Debrids the IP address of the group.

**source srcAddr** — Debrids the source IP address.

**rp rpAddr** — Debrids the specified rendezvous point RP address.
In This Chapter

This chapter provides information about configuring Routing Information Protocol (RIP) parameters.

Topics in this chapter include:

- RIP Overview on page 232
  - RIP Features on page 233
    - RIP Version Types on page 233
    - RIPv2 Authentication on page 233
    - Metrics on page 234
    - Timers on page 234
    - Import and Export Policies on page 234
    - RIP Packet Format on page 235
- RIP Configuration Process Overview on page 238
- Configuration Notes on page 239
RIP Overview

The Routing Information Protocol (RIP) is an interior gateway protocol (IGP) that uses a distance-vector algorithm to determine the best route to a destination, using hop count as the metric. In order for the protocol to provide complete information on routing, every router in the domain must participate in the protocol.

RIP is a routing protocol based on a distance vector (Bellman-Ford) algorithm, which advertises network reachability by advertising prefix/mask and the metric (also known as hop count or cost). RIP selects the route with the lowest metric as the best route. RIP differs from link-state database protocols, such as OSPF and IS-IS, in that RIP advertises reachability information directly and link-state-database-based protocols advertise topology information. Each node is responsible for calculating the reachability information from the topology.

The router software supports RIPv1 and RIPv2. RIPv1, specified in RFC 1058, was written and implemented prior to the introduction of CIDR. It assumes the netmask information for non-local routes, based on the class the route belongs to:

- Class A – 8 bit mask
- Class B – 16 bit mask
- Class C – 24 bit mask

RIPv2 was written after CIDR was developed and transmits netmask information with every route. Because of the support for CIDR routes and other enhancements in RIPv2 such as triggered updates, and authentication, most production networks use RIPv2. However, there are some older systems (hosts and routers) that only support RIPv1, especially when RIP is used simply to advertise default routing information.

RIP is supported on all IP interfaces, including both network and access interfaces.
RIP Features

RIP, a UDP-based protocol, updates its neighbors, and the neighbors update their neighbors, and so on. Each host that uses RIP has a routing process that sends and receives datagrams on UDP port number 520.

Each RIP router advertises all RIP routes periodically via RIP updates. Each update can contain a maximum of 25 route advertisements. This limit is imposed by RIP specifications. RIP can sometimes be configured to send as many as 255 routes per update. The formats of the RIPv1 and RIPv2 updates are slightly different and are shown below. Additionally, RIPv1 updates are sent to a broadcast address, RIPv2 updates can be either sent to a broadcast address. RIPv2 supports subnet masks, a feature that was not available in RIPv1.

A network address of 0.0.0.0 is considered a default route. A default route is used when it is not convenient to list every possible network in the RIP updates, and when one or more closely-connected gateways in the system are prepared to handle traffic to the networks that are not listed explicitly. These gateways create RIP entries for the address 0.0.0.0, as if it were a network to which they are connected.

RIP Version Types

The router allows you to specify the RIP version that will be sent to RIP neighbors and RIP updates that will be accepted and processed. The router allows the following combinations:

- Send only RIPv1 or send only RIPv2 to either the broadcast or send no messages. The default sends RIPv2 formatted messages to the broadcast address.
- Receive only RIPv1, receive only RIPv2, or receive both RIPv1 and RIPv2, or receive none. The default receives both.

RIPv2 Authentication

RIPv2 messages carry more information, which permit the use of a simple authentication mechanism to secure table updates. The router implementation enables the use of a simple password (plain text) or message digest (MD5) authentication.
Metrics

By default, RIP advertises all RIP routes to each peer every 30 seconds. RIP uses a hop count metric to determine the distance between the packet’s source and destination. The metric/cost values for a valid route is 1 through 15. A metric value of 16 (infinity) indicates that the route is no longer valid and should be removed from the router’s routing table.

Each router along the path increments the hop count value by 1. When a router receives a routing update with new or different destination information, the metric increments by 1.

The maximum number of hops in a path is 15. If a router receives a routing update with a metric of 15 and contains a new or modified entry, increasing the metric value by 1 will cause the metric increment to 16 (infinity). Then, the destination is considered unreachable.

The router implementation of RIP uses split horizon with poison reverse to protect from such problems as “counting to infinity”. Split horizon with poison reverse means that routes learned from a neighbor through a given interface are advertised in updates out of the same interface but with a metric of 16 (infinity).

Timers

RIP uses numerous timers to determine how often RIP updates are sent and how long routes are maintained.

- Update — Times the interval between periodic routing updates.
- Timeout — This timer is initialized when a route is established and any time an update message is received for the route. When this timer expires, the route is no longer valid. It is retained in the table for a short time, so that neighbors can be notified that the route has been dropped.
- Flush — When the flush timer expires, the route is removed from the tables.

Import and Export Policies

Routing policies can control the content of the routing tables, the routes that are advertised and the best route to take to reach a destination. Import route policies determine which routes are accepted from RIP neighbors. Export route policies determine which routes are exported from the route table to RIP. By default, RIP does not export routes it has learned to its neighbors.

There are no default routing policies. A policy must be created explicitly and applied to a RIP import or export command.
### RIP Packet Format

The RIP packet format is displayed in **Figure 3**:

![RIP Packet Format](image)

**Figure 3: RIP Packet Format**

A RIP packet consists of the following fields:

- **Command** — Indicates whether the packet is a request or a response message. The request asks the responding system to send all or part of its routing table. The response may be sent in response to a request, or it may be an unsolicited routing update generated by the sender.

- **Version** — The RIP version used. This field can signal different potentially incompatible versions.

- **Must be zero** — Not used in RIPv1. This field provides backward compatibility with pre-standard varieties of RIP. The default value is zero.

- **Address family identifier (AFI)** — The AFI is the type of address. RIP can carry routing information for several different protocols. Each entry in this field has an AFI to indicate the type of address being specified. The IP AFI is 2.

- **Address** — The IP address for the packet.

- **Metric** — Specifies the number of hops to the destination.

- **Mask** — Specifies the IP address mask.

- **Next hop** — Specifies the IP address of the next router along the path to the destination.
RIPv1 Format

There can be between 1 and 25 (inclusive) RIP entries. Figure 4 displays RIPv1 format:

![Figure 4: RIPv1 Format](image)

RIPv2 Format

The RIP packet format is displayed in Figure 5:

![Figure 5: RIPv2 Format](image)

The RIPv2 packets include the following fields:

- Subnet mask — The subnet mask for the entry. If this field is zero, no subnet mask has been specified for the entry.
- Next hop — The IP address of the next hop to forward packets.
Hierarchical Levels

The minimum RIP configuration must define one group and one neighbor. The parameters configured on the global level are inherited by the group and neighbor levels. Parameters can be modified and overridden on a level-specific basis. RIP command hierarchy consists of three levels:

- Global
- Group
- Neighbor

Many of the hierarchical RIP commands can be modified on different levels. The most specific value is used. That is, a RIP group-specific command takes precedence over a global RIP command. A neighbor-specific statement takes precedence over a global RIP and group-specific command; for example, if you modify a RIP neighbor-level command default, the new value takes precedence over group- and global-level settings.
RIP Configuration Process Overview

Figure 6 displays the process to configure RIP parameters.

Figure 6: RIP Configuration and Implementation Flow
Configuration Notes

This section describes RIP configuration caveats.

General

- Before RIP neighbor parameters can be configured, router interfaces must be configured.
- RIP must be explicitly created for each router interface. There are no default RIP instances on a router.
Configuring RIP with CLI

This section provides information to configure Routing Information Protocol (RIP) using the command line interface.

Topics in this section include:

- RIP Configuration Overview on page 242
- Basic RIP Configuration on page 243
- Common Configuration Tasks on page 244
  - Configuring Interfaces on page 245
  - Configuring a Route Policy on page 246
  - Configuring RIP Parameters on page 248
  - Configuring Global-Level Parameters on page 250
  - Configuring Group-Level Parameters on page 251
  - Configuring Neighbor-Level Parameters on page 252
- RIP Configuration Management Tasks on page 253
  - Modifying RIP Parameters on page 253
  - Deleting a Group on page 254
  - Deleting a Neighbor on page 254
RIP Configuration Overview

Preconfiguration Requirements

Configure the following entities before beginning the RIP configuration:

- (Optional) Policy statements should be defined in the `config>router>policy-options` context.

RIP Hierarchy

RIP is configured in the `config>router>rip` context. RIP is not enabled by default. Three hierarchical levels are included in RIP configurations:

- Global
- Group
- Neighbor

Commands and parameters configured on the global level are inherited by the group and neighbor levels although parameters configured on the group and neighbor levels take precedence over global configurations.
Basic RIP Configuration

This section provides information to configure RIP and examples of common configuration tasks. For a router to accept RIP updates, in the `config>router>rip` context, you must define at least one group and one neighbor. A router will ignore updates received from routers on interfaces not configured for RIP. Configuring other RIP commands and parameters are optional.

By default, the local router imports all routes from this neighbor and does not advertise routes. The router receives both RIPv1 and RIPv2 update messages with 25 to 255 route entries per message.

The RIP configuration commands have three primary configuration levels: `rip` for global configurations, group `group-name` for RIP group configurations, and neighbor `ip-int-name` for RIP neighbor configurations. Within the different levels, the configuration commands are identical. For the repeated commands, the command that is most specific to the neighboring router is in effect; that is, neighbor settings have precedence over group settings which have precedence over RIP global settings.

The minimal RIP parameters that need to be configured in the `config>router>rip` context are:

- Group
- Neighbor

The following example displays a basic RIP configuration.

```
ALA-A>config>router>rip# info
-------------------------------------------------------------
   group "RIP-ALA-A"
neighbor "to-ALA-4"
   exit
-------------------------------------------------------------
ALA-A>config>router>rip#
```
Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure RIP and provides the CLI commands.

Configure RIP hierarchically using the global level (applies to all peers), the group level (applies to all peers in peer-group), or the neighbor level (only applies to the specified interface). By default, group members inherit the group’s configuration parameters although a parameter can be modified on a per-member basis without affecting the group-level parameters.

Many of the hierarchical RIP commands can be used on different levels. The most specific value is used. That is, a RIP group-specific command takes precedence over a global RIP command. A neighbor-specific statement takes precedence over a global RIP or group-specific command.

All RIP instances must be explicitly created on each device. Once created, RIP is administratively enabled.

To configure RIP, perform the following tasks:

1. Configure interfaces
2. Configure policy statements (optional)
3. Enable RIP
4. Configure group parameters
5. Configure neighbor parameters
Configuring Interfaces

The following command sequences create a logical IP interface. The logical interface can associate attributes like an IP address, port, Link Aggregation Group (LAG), or the system. For more information about configuring interfaces, refer to the IP Router Configuration Overview chapter.

To configure a network interface:

**CLI Syntax:**

```
config> router
   interface ip-int-name
       address ip-addr[/mask-length|mask] [broadcast {all-ones|host-ones}]
       port port-id
```

The following example displays router interface configuration command usage:

**Example:**

```
config>router> interface “to-ALA-4”
config>router>if$ address 10.10.12.1/24
config>router>if# port 1/1/1
config>router>if# exit
```

The following example displays the IP configuration output showing the interface information.

```
ALA-3>config>router# info
#------------------------------------------
echo "IP Configuration "
#------------------------------------------
   interface "system"
       address 10.10.103/32
exit
   interface "to-ALA-4"
       address 10.10.12.1/24
       port 1/1/1
exit
#------------------------------------------
ALA-3>config>router#
```
Configuring a Route Policy

The import route policy command allows you to filter routes being imported by the local router from its neighbors. If no match is found, the local router does not import any routes.

The export route policy command allows you to determine which routes are exported from the route table to RIP. By default, RIP does not export routes it has learned to its neighbors. If no export policy is specified, non-RIP routes will not be exported from the routing table manager to RIP.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

This section only provides brief instructions to configure route policies. For more details, refer to the Route Policy Overview chapter.

To enter the mode to create or edit route policies, you must enter the `begin` keyword at the `config>router>policy-options` prompt. Other editing commands include:

- The `commit` command saves and enables changes made to route policies during a session.
- The `abort` command discards changes that have been made to route policies during a session.

Use the following CLI syntax to configure a policy to use for the RIP global, group, and neighbor import and export commands.

**CLI Syntax:**

```
cfg-router-policy-options
begin
commit
abort
policy-statement name
description text
default-action {accept|reject}
entry entry-id
description text
action {accept|reject}
from
to
```
Use the following CLI syntax to enter the edit mode:

**CLI Syntax:**

```
config>router> policy-options
   begin
```

The following example displays some commands to configure a policy statement. Policy option commands are configured in the `config>router` context. Use the `commit` command to save the changes.

**Example:**
```
config>router>policy-options# begin
   policy-options# policy-statement"RIP-policy"
   policy-options>policy-statement$ description "this is a
test RIP policy"
   policy-options>policy-statement>default# entry 1
   policy-options>policy-statement>entry$ action accept
   policy-options>policy-statement>entry# exit
   policy-options>policy-statement# default-action reject
   policy-options>policy-statement# exit
   policy-options# commit

ALA-A>config>router>policy-options# info
----------------------------------------------
   policy-statement "RIP-policy"
   description "this is a test RIP policy"
   entry 1
   action accept
   exit
   exit
   exit
   default-action reject
   exit
----------------------------------------------
ALA-A>config>router>policy-options>policy-statement#
```
Configuring RIP Parameters

Use the CLI syntax displayed below for:

- Configuring RIP Parameters on page 248
- Configuring Group-Level Parameters on page 251
- Configuring Neighbor-Level Parameters on page 252

**CLI Syntax:**

```
config>router
    rip
    authentication-key [authentication-key|hash-key
        [hash|hash2]
    authentication-type {none|password|message-digest|message-digest-20}
    check-zero {enable|disable}
    description string
    export policy-name [policy-name ... up to 5 max]
    import policy-name [policy-name ... up to 5 max]
    message-size number
    metric-in metric
    metric-out metric
    preference number
    receive {both|none|version-1|version-2}
    send {broadcast|multicast|none|version-1|both}
    no shutdown
    split-horizon {enable|disable}
    timers update timeout flush

group group-name
    authentication-key [authentication-key|hash-key
        [hash|hash2]
    authentication-type {none|password|message-digest|message-digest-20}
    check-zero {enable|disable}
    description string
    export policy-name [policy-name ... up to 5 max]
    import policy-name [policy-name ... up to 5 max]
    message-size number
    metric-in metric
    metric-out metric
    preference number
    receive {both|none|version-1|version-2}
    send {broadcast|multicast|none|version-1}
    no shutdown
    split-horizon {enable|disable}
    timers update timeout flush
```
neighbor ip-int-name
   authentication-key [authentication-key] hash-key
      [hash|hash2]
   authentication-type {none|password|message-digest|
      message-digest-20}
   check-zero {enable|disable}
   description string
   export policy-name [policy-name ... up to 5 max]
   import policy-name [policy-name ... up to 5 max]
   message-size number
   metric-in metric
   metric-out metric
   preference number
   receive {both|none|version-1|version-2}
   send {broadcast|multicast|none|version-1}
   split-horizon {enable|disable}
   timers update timeout flush
no shutdown
Configuring Global-Level Parameters

Once the RIP protocol instance is created, the `no shutdown` command is not required since RIP is administratively enabled upon creation. Minimally, to enable RIP on a router, at least one group and one neighbor must be configured. There are no default groups or neighbors. Each group and neighbor must be explicitly configured.

NOTE: Careful planning is essential to implement commands that can affect the behavior of global, group, and neighbor-levels. Because the RIP commands are hierarchical, analyze the values that can disable features on a particular level. Use the following CLI syntax to configure global-level RIP parameters:

**CLI Syntax:**
```plaintext
config>router
   rip
   authentication-key [authentication-key|hash-key
   [hash|hash2]
   authentication-type {password|message-digest}
   check-zero {enable|disable}
   export policy-name [policy-name ... up to 5 max]
   import policy-name [policy-name ... up to 5 max]
   message-size number
   metric-in metric
   metric-out metric
   preference number
   receive {both|none|version-1|version-2}
   send {broadcast|multicast|none|version-1|both}
   no shutdown
   split-horizon {enable|disable}
   timers update timeout flush
```

The following example displays global RIP configuration command usage:

**Example:**
```plaintext
config>router# rip
config>router# authentication-type password
config>router# authentication-key test123
config>router# receive both
config>router# split-horizon enable
config>router# timers 300 600 600
config>router# group# exit
```

The following example displays the RIP group configuration:

```plaintext
ALA-A>config>router>rip# info
---------------------------------------------------------------
   authentication-type simple
   authentication-key "ac18651vz1d" hash
   timers 300 600 600
---------------------------------------------------------------
ALA-A>config>router>rip#
```
Configuring Group-Level Parameters

A group is a collection of related RIP peers. The group name should be a descriptive name for the group. Follow your group, name, and ID naming conventions for consistency and to help when troubleshooting faults.

All parameters configured for a group are applied to the group and are inherited by each peer (neighbor), but a group parameter can be overridden on a specific neighbor-level basis. Use the following CLI syntax to configure a group:

**CLI Syntax:**

```
config>router# rip
    group group-name
        authentication-key [authentication-key] hash-key [hash|hash2]
        authentication-type {password|message-digest}
        check-zero {enable|disable}
        description string
        export policy-name [policy-name ...]
        import policy-name [policy-name ...]
        message-size number
        metric-in metric
        metric-out metric
        preference number
        receive {both|none|version-1|version-2}
        send {broadcast|multicast|none|version-1|both}
        no shutdown
        split-horizon {enable|disable}
        timers update timeout flush
```

The following example displays group configuration command usage:

**Example:**

```
config>router# rip
config>router>rip# group headquarters
config>router>rip>group$ description "Mt. View"
config>router>rip>group# no shutdown
```

The following example displays the RIP group configuration:

```
ALA-A>config>router>rip# info
----------------------------------------------
    authentication-type simple
    authentication-key "acl865lvzld" hash
timers 300 600 600
group "headquarters"
    description "Mt. View"
    exit
----------------------------------------------
ALA-A>config>router>rip#
```
Configuring Neighbor-Level Parameters

After you create a group name and assign options, add neighbor interfaces within the same group. All parameters configured for the peer group level are applied to each neighbor, but a group parameter can be overridden on a specific neighbor basis.

Use the following CLI syntax to add a neighbor to a group and define options that override the same group-level command value:

**CLI Syntax:**
```
config>router# rip
group group-name
neighbor ip-int-name
  authentication-key [authentication-key|hash-key
    [hash|hash2] authentication-type {password|message-digest} check-zero {enable|disable} description string export policy-name [policy-name ...] import policy-name [policy-name ...] message-size number metric-in metric metric-out metric preference number receive {both|none|version-1|version-2} send {broadcast|multicast|none|version-1} split-horizon {enable|disable} timers update timeout flush no shutdown
```

The following example displays neighbor configuration command usage:

**Example:**
```
config>router# rip
cfgiurouterrrip# group headquarters1
cfgiurouterrrip-config# group# neighbor ferguson-274
cfgiurouterrrip-config# group# neighbor$ preference 255
cfgiurouterrrip-config# group# neighbor$ send both
cfgiurouterrrip-config# group# neighbor$ split-horizon enable
cfgiurouterrrip-config# group# neighbor$ message-size 255
```

The following example displays the neighbor configured in group “headquarters”.

```
ALA-A>config>router>rip>group>neighbor# info
----------------------------------------------
message-size 255
preference 255
split-horizon enable
no timers
----------------------------------------------
ALA-A>config>router>rip>group>neighbor#
```
RIP Configuration Management Tasks

Examples are provided for the following RIP configuration management tasks:

- Modifying RIP Parameters on page 253
- Deleting a Group on page 254
- Deleting a Neighbor on page 254

Modifying RIP Parameters

Modify, add or remove RIP parameters in the CLI. The changes are applied immediately. For the complete list of CLI commands, refer to Configuring RIP Parameters on page 248.

**CLI Syntax:**
```
config>router# rip
    group group-name
    . . .
    neighbor ip-int-name
    . . .
```

**Example:**
```
config>router>rip# group "headquarters"
config>router>rip>group# neighbor "ferguson-274"
config>router>rip>group>neighbor# import RIPpolicy
config>router>rip>group>neighbor# message-size 150
```

The following example displays the updated parameters:

```
ALA-A>config>router>rip# info
----------------------------------------------
  authentication-type simple
  authentication-key "ac1869lvs1d" hash
  timers 300 600 600
  group "headquarters"
    description "Mt. View"
    neighbor "ferguson-274"
      import "RIPpolicy"
      message-size 150
      preference 255
      split-horizon enable
      no timers
    exit
    exit
----------------------------------------------
ALA-A>config>router>rip#
```
Deleting a Group

A group must be shut down first in order to delete it.

Use the following CLI syntax to shut down and then delete a group:

**CLI Syntax:**

```
config>router# rip
    [no] group group-name
    shutdown
```

**Example:**

```
config>router# rip
    config>router>rip# group "RIP-ALA-3"
    config>router>rip>group# shutdown
    config>router>rip>group# exit
    config>router>rip# no group "RIP-ALA-3"
```

If you try to delete the group without shutting it down first, the following message appears:

```
INFO: RIP #1204 group should be administratively down - virtual router index 1, group RIP-ALA-4
```

Deleting a Neighbor

The neighbor must be shut down before it can be deleted.

Use the following CLI syntax to delete a neighbor:

**CLI Syntax:**

```
config>router# rip
    [no] group group-name
    [no] neighbor ip-int-name
    shutdown
```

**Example:**

```
config>router# rip
    config>router>rip# group "RIP-ALA-4"
    config>router>rip>group# neighbor "to-ALA-3"
    config>router>rip>group>neighbor# shutdown
    config>router>rip>group>neighbor# exit
    config>router>rip>group# no neighbor "to-ALA-3"
```

If you try to delete the neighbor before it is shut down, the following message appears:

```
INFO: RIP #1101 neighbor should be administratively down - virtual router index
```
RIP Command Reference

Command Hierarchies

• Configuration Commands on page 255
  → Group Commands on page 256
  → Neighbor Commands on page 257
• Show RIP Commands on page 258
• Clear RIP Commands on page 258
• Debug RIP Commands on page 258

Configuration Commands

```
config
  - router router-name
    - [no] rip
      - authentication-key [authentication-key | hash-key] [hash | hash2]
      - no authentication-key
      - authentication-type {none | password | message-digest | message-digest-20}
      - no authentication-type
      - check-zero {enable | disable}
      - no check-zero
      - description string
      - no description
      - export policy-name [policy-name ...(up to 5 max)]
      - no export
      - export-limit number [log percentage]
      - no export-limit
      - import policy-name [policy-name ...(up to 5 max)]
      - no import
      - message-size max-num-of-routes
      - no message-size
      - metric-in metric
      - no metric-in
      - metric-out metric
      - no metric-out
      - preference preference
      - no preference
      - receive receive-type
      - no receive
      - send send-type
      - no send
      - [no] shutdown
      - split-horizon {enable | disable}
      - no split-horizon
      - timers update timeout flush
      - no timers
```
Group Commands

```
config
  — router router-name
  — [no] rip
  — [no] group group-name
    — authentication-key [authentication-key | hash-key] [hash | hash2]
    — no authentication-key
    — authentication-type {none | password | message-digest | message-digest-20}
    — no authentication-type
    — check-zero {enable | disable}
    — no check-zero
    — description description-string
    — no description
    — export policy-name [policy-name ...(up to 5 max)]
    — no export
    — import policy-name [policy-name ...(up to 5 max)]
    — no import
    — message-size max-num-of-routes
    — no message-size
    — metric-in metric
    — no metric-in
    — metric-out metric
    — no metric-out
    — preference preference
    — no preference
    — receive receive-type
    — no receive
    — send send-type
    — no send
    — [no] shutdown
    — split-horizon {enable | disable}
    — no split-horizon
    — timers update timeout flush
    — no timers
```
Neighbor Commands

```text
config
  — router router-name
  — [no] rip
  — [no] group group-name
  — [no] neighbor ip-int-name
    — authentication-key [authentication-key | hash-key] [hash | hash2]
    — no authentication-key
    — authentication-type {none | password | message-digest}
    — no authentication-type
    — check-zero {enable | disable}
    — no check-zero
    — description description-string
    — no description
    — export policy-name [policy-name ...(up to 5 max)]
    — no export
    — import policy-name [policy-name ...(up to 5 max)]
    — no import
    — message-size max-num-of-routes
    — no message-size
    — metric-in metric
    — no metric-in
    — metric-out metric
    — no metric-out
    — preference preference
    — no preference
    — receive receive-type
    — no receive
    — send send-type
    — no send
    — [no] shutdown
    — split-horizon {enable | disable}
    — no split-horizon
    — timers update timeout flush
    — no timers
```
RIP Command Reference

Show RIP Commands

show
  — router
    — rip
      — database [ip-prefix [mask] [longer] [peer ip-address] [detail]
      — group [name] [detail]
      — neighbors [ip-int-name | ip-addr] [detail] [advertised-routes]
      — peer [interface-name]
      — statistics [ip-int-name | ip-addr]

Clear RIP Commands

clear
  — router
    — rip
      — database
      — statistics [neighbor ip-int-name | ip-addr]

Debug RIP Commands

default
  — router
    — rip
      — [no] auth [neighbor ip-int-name | ip-addr]
      — [no] error [neighbor ip-int-name | ip-addr]
      — [no] events [neighbor ip-int-name | ip-addr]
      — [no] holddown [neighbor ip-int-name | ip-addr]
      — [no] packets [neighbor ip-int-name | ip-addr]
      — [no] request [neighbor ip-int-name | ip-addr]
      — [no] trigger [neighbor ip-int-name | ip-addr]
      — [no] updates [neighbor ip-int-name | ip-addr]
RIP Configuration Commands

Generic Commands

description

Syntax  
description  string  
no description

Context  
config>router>rip>group  group-name
config>router>rip>group  group-name>neighbor  ip-int-name

Description  
This command creates a text description stored in the configuration file for a configuration context.

The description command associates a text string with a configuration context to help identify the context in the configuration file.

The no form of the command removes any description string from the context.

Default  
no description — no description associated with the configuration context.

Parameters  
string — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

shutdown

Syntax  
[no] shutdown

Context  
config>router>rip
config>router>rip>group  group-name
config>router>rip>group  group-name>neighbor  ip-int-name

Description  
This command administratively disables an entity. Downing an entity does not change, reset or remove any configuration settings or statistics. Many objects must be shutdown before they may be deleted.

The shutdown command administratively downs an entity. Administratively downing an entity changes the operational state of the entity to down and the operational state of any entities contained within the administratively down entity.

Unlike other commands and parameters where the default state will not be indicated in the configuration file, shutdown and no shutdown are always indicated in system generated configuration files.

The no form of the command puts an entity into the administratively enabled state.

Special Cases  
RIP Global — In the config>router>rip context, the shutdown command administratively enables/disables the RIP protocol instance. If RIP is globally shutdown, then all RIP group and neighbor interfaces transition to the operationally down state. Routes learned from a neighbor that is shutdown are immediately removed
from the RIP database and route table manager (RTM). A RIP protocol instance is administratively enabled by default.

**RIP Group** — In the config>router>rip>group group-name context, the `shutdown` command administratively enables/disables the RIP group. If a RIP group is shutdown, all member neighbor interfaces transition to the operationally down state. Routes learned from a neighbor that is shutdown are immediately removed from the RIP database and route table manager (RTM). A RIP group is administratively enabled by default.

**RIP Neighbor** — In the config>router>rip>group group-name>neighbor ip-int-name context, the `shutdown` command administratively enables/disables the RIP neighbor interface. If a RIP neighbor is shutdown, the neighbor interface transitions to the operationally down state. Routes learned from a neighbor that is shutdown are immediately removed from the RIP database and route table manager (RTM). A RIP neighbor interface is administratively enabled by default.
RIP Commands

rip

Syntax  [no] rip
Context  config>router
Description  This command creates the context to configure the RIP protocol instance.
When a RIP instance is created, the protocol is enabled by default. To start or suspend execution of the RIP
protocol without affecting the configuration, use the [no] shutdown command.
The no form of the command deletes the RIP protocol instance removing all associated configuration
parameters.
Default  no rip — No RIP protocol instance defined.

authentication-key

Syntax  authentication-key [authentication-key | hash-key] [hash | hash2]
no authentication-key
Context  config>router>rip
       config>router>rip>group group-name
       config>router>rip>group group-name>neighbor ip-int-name
Description  This command sets the authentication password to be passed between RIP neighbors.
The authentication type and authentication key must match exactly for the RIP message to be considered
authentic and processed.
The no form of the command removes the authentication password from the configuration and disables
authentication.
Default  no authentication-key — No authentication key configured.
Parameters  authentication-key — The authentication key. Allowed values are any string up to 16 characters long
composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces,
etc.), the entire string must be enclosed within double quotes.
hash-key — The hash key. The key can be any combination of ASCII characters up to 33 characters in length
(encrypted). If spaces are used in the string, enclose the entire string in quotation marks
(" ").
    This is useful when a user must configure the parameter, but, for security purposes, the actual
    unencrypted key value is not provided.
hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is
assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in
the configuration file with the hash parameter specified.
hash2 — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.

**authentication-type**

**Syntax**

```
authentication-type {none|password|message-digest|message-digest-20}
no authentication-type
```

**Context**

```
config>router>rip
config>router>rip>group group-name
config>router>rip>group group-name>neighbor ip-int-name
```

**Description**

This command sets the type of authentication to be used between RIP neighbors.

The type and password must match exactly for the RIP message to be considered authentic and processed.

The no form of the command removes the authentication type from the configuration and effectively disables authentication.

**Default**

no authentication-type — No authentication enabled.

**Parameters**

- **none** — The none parameter explicitly disables authentication at a given level (global, group, neighbor). If the command does not exist in the configuration, the parameter is inherited.

- **password** — Specify password to enable simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple password authentication is enabled.

- **message-digest** — Configures 16 byte message digest for MD5 authentication. If this option is configured, then at least one message-digest-key must be configured.

- **message-digest-20** — Configures 20 byte message digest for MD5 authentication in accordance with RFC 2082, RIPv2 MD5 Authentication. If this option is configured, then at least one message-digest-key must be configured.

**check-zero**

**Syntax**

```
check-zero {enable | disable}
no check-zero
```

**Context**

```
config>router>rip
config>router>rip>group group-name
config>router>rip>group group-name>neighbor ip-int-name
```

**Description**

This command enables checking for zero values in fields specified to be zero by the RIPv1 and RIPv2 specifications.

The check-zero enable command enables checking of the mandatory zero fields in the RIPv1 and RIPv2 specifications and rejecting non-compliant RIP messages.

The check-zero disable command disables this check and allows the receipt of RIP messages even if the mandatory zero fields are non-zero.
This configuration parameter can be set at three levels: global level (applies to all groups and neighbor interfaces), group level (applies to all neighbor interfaces in the group) or neighbor level (only applies to the specified neighbor interface). The most specific value is used. In particular if no value is set (no check-zero), the setting from the less specific level is inherited by the lower level.

The no form of the command removes the check-zero command from the configuration.

Special Cases

RIP Global — By default, check-zero is disabled at the global RIP instance level.

Parameters

enable — Specifies reject RIP messages which do not have zero in the RIPv1 and RIPv2 mandatory fields.
disable — Specifies allows receipt of RIP messages which do not have the mandatory zero fields reset.

export

Syntax export policy-name [policy-name ...up to 5 max]
no export

Context config>router>rip
config>router>rip>group group-name
config>router>rip>group group-name>neighbor ip-int-name

Description

This command specifies the export route policies used to determine which routes are exported to RIP.

If no export policy is specified, non-RIP routes will not be exported from the routing table manager to RIP.
RIP-learned routes will be exported to RIP neighbors.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The no form of the command removes all policies from the configuration.

Default no export — No export route policies specified.

Parameters policy-name — The export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

export-limit

Syntax export-limit number [log percentage]
no export-limit

Context config>router>rip

Description

This command configures the maximum number of routes (prefixes) that can be exported into RIP from the route table.

The no form of the command removes the parameters from the configuration.
RIP Commands

Default no export-limit, the export limit for routes or prefixes is disabled.

Parameters

- number — Specifies the maximum number of routes (prefixes) that can be exported into RIP from the route table.
  - Values 1 — 4294967295

- log percentage — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.
  - Values 1 — 100

group

Syntax [no] group group-name

Context config>router>rip

Description This command creates a context for configuring a RIP group of neighbor interfaces.

RIP groups are a way of logically associating RIP neighbor interfaces to facilitate a common configuration for RIP interfaces.

The no form of the command deletes the RIP neighbor interface group. Deleting the group will also remove the RIP configuration of all the neighbor interfaces currently assigned to this group.

Default no group — No group of RIP neighbor interfaces defined.

Parameters group-name — The RIP group name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

import

Syntax import policy-name [policy-name ...up to 5 max]
    no import

Context config>router>rip
    config>router>rip>group group-name
    config>router>rip>group group-name>neighbor ip-int-name

Description This command configures import route policies to determine which routes are accepted from RIP neighbors.

If no import policy is specified, RIP accepts all routes from configured RIP neighbors. Import policies can be used to limit or modify the routes accepted and their corresponding parameters and metrics.

If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The no form of the command removes all policies from the configuration.

Default no import — No import route policies specified.
Parameters  

*policy-name* — The import route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.

### message-size

**Syntax**  
message-size  
max-num-of-routes  
no message-size

**Context**  
config>router>rip
config>router>rip>group  
group-name
config>router>rip>group  
group-name>neighbor  
ip-int-name

**Description**  
This command configures the maximum number of routes per RIP update message.

The *no* form of the command reverts to the default value.

**Default**  
message-size 25 — A maximum of 25 routes per RIP update message.

**Parameters**  
max-num-of-routes — The maximum number of RIP routes per RIP update message expressed as a decimal integer.

**Values**  
25 — 255

### metric-in

**Syntax**  
metric-in  
metric  
no metric-in

**Context**  
config>router>rip
config>router>rip>group  
group-name
config>router>rip>group  
group-name>neighbor  
ip-int-name

**Description**  
This command configures the metric added to routes received from a RIP neighbor.

When applying an export policy to a RIP configuration, the policy overrides the metric values determined through calculations involving the metric-in and metric-out values.

The *no* form of the command reverts to the default value.

**Default**  
metric-in 1 — Add 1 to the metric of routes received from a RIP neighbor.

**Parameters**  
metric — The value added to the metric of routes received from a RIP neighbor expressed as a decimal integer.

**Values**  
1 — 16
RIP Commands

metric-out

Syntax  
metric-out metric
no metric-out

Context  
config>router>rip
config>router>rip>group group-name
config>router>rip>group group-name>neighbor ip-int-name

Description  
This command configures the metric assigned to routes exported into RIP and advertised to RIP neighbors.

When applying an export policy to a RIP configuration, the policy overrides the metric values determined through calculations involving the metric-in and metric-out values.

The no form of the command reverts to the default value.

Default  
metric-out 1 — Routes exported from non-RIP sources are given a metric of 1.

Parameters  
metric — The value added to the metric for routes exported into RIP and advertised to RIP neighbors expressed as a decimal integer.

Values  
1 — 16

neighbor

Syntax  
[no] neighbor ip-int-name

Context  
config>router>rip>group group-name

Description  
This command creates a context for configuring a RIP neighbor interface.

By default, interfaces are not activated in any interior gateway protocol, such as RIP, unless explicitly configured.

The no form of the command deletes the RIP interface configuration for this interface. The shutdown command in the config>router>rip>group group-name>neighbor ip-int-name context can be used to disable an interface without removing the configuration for the interface.

Default  
no neighbor — No RIP interfaces defined.

Parameters  
ip-int-name — The IP interface name. Interface names must be unique within the group of defined IP interfaces for config router interface and config service ies interface commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured, an error message will be returned.
preference

**Syntax**

```
preference preference
no preference
```

**Context**

```
config>router>rip
cfg-router>rip>group group-name
config>router>rip>group group-name>neighbor ip-int-name
```

**Description**

This command configures the preference for RIP routes.

A route can be learned by the router from different protocols in which case the costs are not comparable. When this occurs the preference is used to decide which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in Table 7. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the `ecmp` in the `config>router` context.

The `no` form of the command reverts to the default value.

**Default**

- `preference 100` — Preference of 100 for RIP routes.

**Parameters**

- `preference` — The preference for RIP routes expressed as a decimal integer. Defaults for different route types are listed in Table 7.

**Table 7: Route Preference Defaults by Route Type**

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Preference</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct attached</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Static routes</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF internal</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 internal</td>
<td>15</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 internal</td>
<td>18</td>
<td>Yes</td>
</tr>
<tr>
<td>RIP</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF external</td>
<td>150</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 external</td>
<td>160</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 external</td>
<td>165</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Values**

- 0 — 255
RIP Commands

receive

Syntax  receive {both | none | version-1 | version-2}

        no receive

Context  config>router>rip
         config>router>rip>group group-name
         config>router>rip>group group-name>neighbor ip-int-name

Description  This command configures the type(s) of RIP updates that will be accepted and processed.

        If both or version-2 is specified, the RIP instance listens for and accepts packets sent to the broadcast and multicast (224.0.0.9) addresses.

        If version-1 is specified, the router only listens for and accept packets sent to the broadcast address.

        This control can be issued at the global, group or interface level. The default behavior is to accept and process both RIPv1 and RIPv2 messages.

        The no form of the command reverts to the default value.

Default  receive both

Parameters  both — Specifies that RIP updates in either version 1 or version 2 format will be accepted.

none — Specifies that RIP updates will not be accepted.

version-1 — Specifies that RIP updates in version 1 format only will be accepted.

version-2 — Specifies that RIP updates in version 2 format only will be accepted.

send

Syntax  send {broadcast | multicast | none | version-1}

        no send

Context  config>router>rip
         config>router>rip>group group-name
         config>router>rip>group group-name>neighbor ip-int-name

Description  This command specifies the type of RIP messages sent to RIP neighbors.

        If version-1 is specified, the router need only listen for and accept packets sent to the broadcast address.

        This control can be issued at the global, group or interface level.

        The no form of the command reverts to the default value.

Default  send broadcast — RIPv2 formatted messages will be sent to the broadcast address.

Parameters  broadcast — Specifies send RIPv2 formatted messages to the broadcast address.

multicast — Specifies send RIPv2 formatted messages to the multicast address.

none — Specifies not to send any RIP messages (i.e. silent listener).

version-1 — Specifies send RIPv1 formatted messages to the broadcast address.
split-horizon

Syntax  

split-horizon {enable | disable}
no split-horizon

Context  

config>router>rip
config>router>rip>group group-name
config>router>rip>group group-name>neighbor ip-int-name

Description  

This command enables the use of split-horizon.

RIP uses split-horizon with poison-reverse to protect from such problems as “counting to infinity”. Split-
horizon with poison reverse means that routes learned from a neighbor through a given interface are
advertised in updates out of the same interface but with a metric of 16 (infinity).

The split-horizon disable command enables split horizon without poison reverse. This allows the routes to
be re-advertised on interfaces other than the interface that learned the route, with the advertised metric
equaling an increment of the metric-in value.

This configuration parameter can be set at three levels: global level (applies to all groups and neighbor
interfaces), group level (applies to all neighbor interfaces in the group) or neighbor level (only applies to the
specified neighbor interface). The most specific value is used. In particular if no value is set (no split-
horizon), the setting from the less specific level is inherited by the lower level.

The no form of the command disables split horizon command which allows the lower level to inherit the
setting from an upper level.

Default  

enabled

Parameters  

enable — Specifies enable split horizon and poison reverse.

disable — Specifies disable split horizon allowing routes to be re-advertised on the same interface on which
they were learned with the advertised metric incremented by the metric-in value.

timers

Syntax  

timers update timeout flush
no timers

Context  

config>router>rip
config>router>rip>group group-name
config>router>rip>group group-name>neighbor ip-int-name

Description  

This command configures values for the update, timeout and flush RIP timers.

The RIP update timer determines how often RIP updates are sent.

If the route is not updated by the time the RIP timeout timer expires, the route is declared invalid but is
maintained in the RIP database.

The RIP flush timer determines how long a route is maintained in the RIP database after it has been declared
invalid. Once the flush timer expires, the route is removed from the RIP database.

The no form of the command reverts to the default values.
RIP Commands

**Default**  
**timers 30 180 120** — RIP update timer set to 30 seconds, timeout timer to 180 seconds and flush timer to 120 seconds.

**Parameters**  
**update** — The RIP update timer value in seconds expressed as a decimal integer.

**Values**  
1 — 600

**timeout** — The RIP timeout timer value in seconds expressed as a decimal integer.

**Values**  
1 — 1200

**flush** — The RIP flush timer value in seconds expressed as a decimal integer.

**Values**  
1 — 1200
Show Commands

database

Syntax  
database [ip-prefix [mask] [longer] [peer ip-address]]

Context  
show->router>rip

Description  
This command displays the routes in the RIP database.

Output  
RIP Database Output — The following table describes the RIP route database output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The RIP destination for the route.</td>
</tr>
<tr>
<td>Peer</td>
<td>The router ID of the peer router.</td>
</tr>
<tr>
<td>NextHop</td>
<td>The IP address of the next hop.</td>
</tr>
<tr>
<td>Metric</td>
<td>The hop count to rate the value of different hops.</td>
</tr>
<tr>
<td>Tag</td>
<td>The value to distinguish between internal routes (learned by RIP) and external routes (learned from other protocols).</td>
</tr>
<tr>
<td>TTL</td>
<td>Displays how many seconds the specific route will remain in the routing table. When an entry reaches 0, it is removed from the routing table.</td>
</tr>
<tr>
<td>Valid</td>
<td>Yes — The route is valid.</td>
</tr>
</tbody>
</table>

Valid | No — The route is not valid. |

Sample Output

A:ALA-A# show rip database

RIP Route Database

<table>
<thead>
<tr>
<th>Destination</th>
<th>Peer</th>
<th>NextHop</th>
<th>Metric</th>
<th>Tag</th>
<th>TTL</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>180.0.0.10/32</td>
<td>180.1.7.15</td>
<td>0.0.0.0</td>
<td>2</td>
<td>0x0000</td>
<td>163</td>
<td>No</td>
</tr>
<tr>
<td>180.0.0.10/32</td>
<td>180.1.8.14</td>
<td>0.0.0.0</td>
<td>2</td>
<td>0x0000</td>
<td>179</td>
<td>No</td>
</tr>
<tr>
<td>180.0.0.14/32</td>
<td>180.1.8.14</td>
<td>0.0.0.0</td>
<td>1</td>
<td>0x0000</td>
<td>179</td>
<td>Yes</td>
</tr>
<tr>
<td>180.0.6.0/24</td>
<td>180.1.7.15</td>
<td>0.0.0.0</td>
<td>11</td>
<td>0x2002</td>
<td>163</td>
<td>No</td>
</tr>
<tr>
<td>180.0.6.0/24</td>
<td>180.1.8.14</td>
<td>0.0.0.0</td>
<td>11</td>
<td>0x2002</td>
<td>179</td>
<td>No</td>
</tr>
<tr>
<td>180.0.7.0/24</td>
<td>180.1.7.15</td>
<td>0.0.0.0</td>
<td>11</td>
<td>0x2002</td>
<td>163</td>
<td>No</td>
</tr>
<tr>
<td>180.1.5.0/24</td>
<td>180.1.7.15</td>
<td>0.0.0.0</td>
<td>2</td>
<td>0x0000</td>
<td>151</td>
<td>Yes</td>
</tr>
<tr>
<td>180.1.5.0/24</td>
<td>180.1.8.14</td>
<td>0.0.0.0</td>
<td>1</td>
<td>0x0000</td>
<td>167</td>
<td>No</td>
</tr>
<tr>
<td>180.100.17.16/30</td>
<td>180.1.7.15</td>
<td>0.0.0.0</td>
<td>2</td>
<td>0x0000</td>
<td>151</td>
<td>No</td>
</tr>
<tr>
<td>180.100.17.16/30</td>
<td>180.1.8.14</td>
<td>0.0.0.0</td>
<td>2</td>
<td>0x0000</td>
<td>167</td>
<td>No</td>
</tr>
</tbody>
</table>
group

**Syntax**

```
group [group-name] [detail]
```

**Context**

`show>router>rip`

**Description**

Display RIP group information.

**Parameters**

- `group-name` — Displays RIP group information for the specified group.
- `detail` — Displays detailed RIP group information.

**Output**

**Standard RIP Group Output** — The following table describes the standard command output fields for a RIP group.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>The RIP group name.</td>
</tr>
<tr>
<td>Adm</td>
<td><strong>Down</strong> — The RIP group is administratively down.</td>
</tr>
<tr>
<td></td>
<td><strong>Up</strong> — The RIP group is administratively up.</td>
</tr>
<tr>
<td>Opr</td>
<td><strong>Down</strong> — The RIP group is operationally down.</td>
</tr>
<tr>
<td></td>
<td><strong>Up</strong> — The RIP group is operationally up.</td>
</tr>
<tr>
<td>Send Mode</td>
<td><strong>Bcast</strong> — Specifies that RIPv2 formatted messages are sent to the broadcast address.</td>
</tr>
<tr>
<td></td>
<td><strong>Mcast</strong> — Specifies that RIPv2 formatted messages are sent to the multicast address.</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong> — Specifies that no RIP messages are sent (i.e., silent listener)</td>
</tr>
<tr>
<td></td>
<td><strong>RIPv1</strong> — Specifies that RIPv1 formatted messages are sent to the broadcast address.</td>
</tr>
<tr>
<td>Recv Mode</td>
<td><strong>Both</strong> — Specifies that RIP updates in either version 1 or version 2 format will be accepted.</td>
</tr>
<tr>
<td></td>
<td><strong>None</strong> — Specifies that RIP updates will not be accepted.</td>
</tr>
<tr>
<td></td>
<td><strong>RIPv1</strong> — Specifies that RIP updates in version 1 format only will be accepted.</td>
</tr>
<tr>
<td></td>
<td><strong>RIPv2</strong> — Specifies that RIP updates in version 2 format only will be accepted.</td>
</tr>
<tr>
<td>Metric In</td>
<td>The metric value added to routes received from a RIP neighbor.</td>
</tr>
</tbody>
</table>
Sample Standard RIP Group Output

A:ALA-A# show router rip group

RIP Groups

<table>
<thead>
<tr>
<th>Group</th>
<th>Adm Mode</th>
<th>Opr Mode</th>
<th>Send Mode</th>
<th>Recv Mode</th>
<th>Metric In</th>
</tr>
</thead>
<tbody>
<tr>
<td>rip-group</td>
<td>Up</td>
<td>Down</td>
<td>BCast</td>
<td>Both</td>
<td>1</td>
</tr>
</tbody>
</table>

A:ALA-A#

Sample Detailed Output

A:ALA-A# show router rip group detail

RIP groups (Detail)

Group "rip-group"

Description : No Description Available
Admin State : Up                  Oper State : Down
Send Mode : Broadcast              Receive Mode : Both
Metric In : 1                      Metric Out : 1
Split Horizon : Enabled            Check Zero : Disabled
Message Size : 25                  Preference : 100
Auth. Type : None                   Update Timer : 30
Timeout Timer : 180                Flush Timer : 120
Export Policies:
None
Import Policies:
None

A:ALA-A#

neighbors

Syntax neighbors [ip-addr | ip-int-name] [advertised-routes | detail]

Context show>router>rip

Description Displays RIP neighbor interface information.

Parameters ip-addr | ip-int-name — Displays information for the specified IP interface.

   Default all neighbor interfaces

advertised-routes — Displays the routes advertised to RIP neighbors. If no neighbors are specified, then all routes advertised to all neighbors are displayed. If a specific neighbor is given then only routes advertised to the given neighbor/interface are displayed.

   Default display RIP information
Output

**Standard RIP Neighbor Output** — The following table describes the standard command output fields for a RIP group.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>The RIP neighbor interface name.</td>
</tr>
<tr>
<td>Adm</td>
<td>Down — The RIP neighbor interface is administratively down.</td>
</tr>
<tr>
<td></td>
<td>Up — The RIP neighbor interface is administratively up.</td>
</tr>
<tr>
<td>Opr</td>
<td>Down — The RIP neighbor interface is operationally down.</td>
</tr>
<tr>
<td></td>
<td>Up — The RIP neighbor interface is operationally up.</td>
</tr>
<tr>
<td>Primary IP</td>
<td>The Primary IP address of the RIP neighbor interface.</td>
</tr>
<tr>
<td>Send Mode</td>
<td>Bcast — Specifies that RIPv2 formatted messages are sent to the broadcast</td>
</tr>
<tr>
<td></td>
<td>address.</td>
</tr>
<tr>
<td></td>
<td>Mcast — Specifies that RIPv2 formatted messages are sent to the multicast</td>
</tr>
<tr>
<td></td>
<td>address.</td>
</tr>
<tr>
<td></td>
<td>None — Specifies that no RIP messages are sent (i.e., silent listener).</td>
</tr>
<tr>
<td></td>
<td>RIPv1 — Specifies that RIPv1 formatted messages are sent to the broadcast</td>
</tr>
<tr>
<td></td>
<td>address.</td>
</tr>
<tr>
<td>Recv Mode</td>
<td>Both — Specifies that RIP updates in either version 1 or version 2 format</td>
</tr>
<tr>
<td></td>
<td>will be accepted.</td>
</tr>
<tr>
<td></td>
<td>None — Specifies that RIP updates will not be accepted.</td>
</tr>
<tr>
<td></td>
<td>RIPv1 — Specifies that RIP updates in version 1 format only are accepted.</td>
</tr>
<tr>
<td></td>
<td>RIPv2 — Specifies that RIP updates in version 2 format only are accepted.</td>
</tr>
<tr>
<td>Metric In</td>
<td>The metric added to routes received from a RIP neighbor.</td>
</tr>
</tbody>
</table>

Sample Output

```
A:ALA-A# show router rip neighbor
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>Adm</th>
<th>Opr</th>
<th>Primary IP</th>
<th>Send Mode</th>
<th>Recv Mode</th>
<th>Metric In</th>
</tr>
</thead>
<tbody>
<tr>
<td>router-2/1</td>
<td>Up</td>
<td>Up</td>
<td>10.0.3.12</td>
<td>None</td>
<td>Both</td>
<td>1</td>
</tr>
<tr>
<td>router-2/2</td>
<td>Up</td>
<td>Up</td>
<td>10.0.5.12</td>
<td>BCast</td>
<td>Both</td>
<td>1</td>
</tr>
<tr>
<td>router-2/3</td>
<td>Up</td>
<td>Up</td>
<td>10.0.6.12</td>
<td>BCast</td>
<td>Both</td>
<td>1</td>
</tr>
<tr>
<td>router-2/5</td>
<td>Up</td>
<td>Up</td>
<td>10.0.9.12</td>
<td>BCast</td>
<td>Both</td>
<td>1</td>
</tr>
<tr>
<td>router-2/6</td>
<td>Up</td>
<td>Up</td>
<td>10.0.17.12</td>
<td>None</td>
<td>Both</td>
<td>1</td>
</tr>
<tr>
<td>router-2/7</td>
<td>Up</td>
<td>Up</td>
<td>10.0.16.12</td>
<td>None</td>
<td>Both</td>
<td>1</td>
</tr>
</tbody>
</table>
### Output Details

**Detailed RIP Neighbor Output** — The following table describes the standard command output fields for a RIP group.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>The RIP neighbor name.</td>
</tr>
<tr>
<td>Description</td>
<td>The RIP neighbor description. No Description Available indicates no description is configured.</td>
</tr>
<tr>
<td>Primary IP</td>
<td>The RIP neighbor interface primary IP address.</td>
</tr>
<tr>
<td>Group</td>
<td>The RIP group name of the neighbor interface.</td>
</tr>
<tr>
<td>Admin State</td>
<td>Down — The RIP neighbor interface is administratively down.</td>
</tr>
<tr>
<td></td>
<td>Up — The RIP neighbor interface is administratively up.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down — The RIP neighbor interface is operationally down.</td>
</tr>
<tr>
<td></td>
<td>Up — The RIP neighbor interface is operationally up.</td>
</tr>
<tr>
<td>Send Mode</td>
<td>Bcast — Specifies that RIPv2 formatted messages are sent to the broadcast address.</td>
</tr>
<tr>
<td></td>
<td>Mcast — Specifies that RIPv2 formatted messages are sent to the multicast address.</td>
</tr>
<tr>
<td></td>
<td>None — Specifies that no RIP messages are sent (i.e., silent listener).</td>
</tr>
<tr>
<td></td>
<td>RIPv1 — Specifies that RIPv1 formatted messages are sent to the broadcast address.</td>
</tr>
<tr>
<td>Recv Mode</td>
<td>Both — Specifies that RIP updates in either version 1 or version 2 format will be accepted.</td>
</tr>
<tr>
<td></td>
<td>None — Specifies that RIP updates will not be accepted.</td>
</tr>
<tr>
<td></td>
<td>RIPv1 — Specifies that RIP updates in version 1 format only will be accepted.</td>
</tr>
<tr>
<td></td>
<td>RIPv2 — Specifies that RIP updates in version 2 format only will be accepted.</td>
</tr>
<tr>
<td>Metric In</td>
<td>The metric value added to routes received from a RIP neighbor.</td>
</tr>
<tr>
<td>Metric Out</td>
<td>The value added to routes exported into RIP and advertised to RIP neighbors.</td>
</tr>
<tr>
<td>Split Horizon</td>
<td>Disabled — Split horizon disabled for the neighbor.</td>
</tr>
<tr>
<td></td>
<td>Enabled — Split horizon and poison reverse enabled for the neighbor.</td>
</tr>
</tbody>
</table>
Show Commands

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Zero</td>
<td><strong>Disabled</strong> – Checking of the mandatory zero fields in the RIPv1 and RIPv2 specifications are not checked allowing receipt of RIP messages even if mandatory zero fields are non-zero for the neighbor.</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled</strong> – checking of the mandatory zero fields in the RIPv1 and RIPv2 specifications and rejecting non-compliant RIP messages is enabled for the neighbor.</td>
</tr>
<tr>
<td>Message Size</td>
<td>The maximum number of routes per RIP update message.</td>
</tr>
<tr>
<td>Preference</td>
<td>The preference of RIP routes from the neighbor.</td>
</tr>
<tr>
<td>Auth. Type</td>
<td>Specifies the authentication type.</td>
</tr>
<tr>
<td>Update Timer</td>
<td>The current setting of the RIP update timer value expressed in seconds.</td>
</tr>
<tr>
<td>Timeout Timer</td>
<td>The current RIP timeout timer value expressed in seconds.</td>
</tr>
<tr>
<td>Export Policies</td>
<td>The export route policy that is used to determine routes advertised to all peers.</td>
</tr>
<tr>
<td>Import Policies</td>
<td>The import route policy that is used to determine which routes are accepted from RIP neighbors.</td>
</tr>
</tbody>
</table>

Sample Detailed Output

A:ALA-A# show router rip neighbor detail
-----------------------------------------------------------------------------------------------
RIP Neighbors (Detail)
-----------------------------------------------------------------------------------------------
Neighbor "router-2/7"
-----------------------------------------------------------------------------------------------
Description : No Description Available
Primary IP   : 10.0.16.12          Group : seven
Admin State  : Up               Oper State : Up
Send Mode    : None              Receive Mode : Both
Metric In     : 1                 Metric Out : 1
Split Horizon : Enabled          Check Zero : disabled
Message Size  : 25               Preference : 100
Auth. Type    : None              Update Timer : 3
Timeout Timer : 6                 Flush Timer : 6
Export Policies:
    Rip2Rip
    direct2Rip
Import Policies:
    None
-----------------------------------------------------------------------------------------------
A:ALA-A#
Sample Output

A:ALA-A# show router rip neighbors interface advertised-routes

RIP Advertised Routes

<table>
<thead>
<tr>
<th>Destination</th>
<th>Interface</th>
<th>NextHop</th>
<th>Metric</th>
<th>Tag</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>180.0.0.2/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>10</td>
<td>0x2002</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.5/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>10</td>
<td>0x2002</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.8/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>10</td>
<td>0x2002</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.9/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>10</td>
<td>0x2002</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.10/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>10</td>
<td>0x2002</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.11/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>10</td>
<td>0x2002</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.12/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>1</td>
<td>0x0000</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.13/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>10</td>
<td>0x2002</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.14/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>16</td>
<td>0x0000</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.15/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>2</td>
<td>0x0000</td>
<td>n/a</td>
</tr>
<tr>
<td>180.0.0.16/32</td>
<td>180.1.8.12</td>
<td>0.0.0.0</td>
<td>3</td>
<td>0x0000</td>
<td>n/a</td>
</tr>
</tbody>
</table>

No. of Advertised Routes: 11

A:ALA-A#

peer

Syntax peer [ip-int-name]

Context show>router>rip

Description Displays RIP peer information.

Parameters ip-int-name — Displays peer information for peers on the specified IP interface.

Default display peers for all interfaces

Output RIP Peer Output — The following table describes the command output fields for a RIP peer.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer IP Addr</td>
<td>The IP address of the peer router.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The peer interface name.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of RIP running on the peer.</td>
</tr>
<tr>
<td>Last Update</td>
<td>The number of days since the last update.</td>
</tr>
<tr>
<td>No. of Peers</td>
<td>The number of RIP peers.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-A# show router rip peers
### RIP Peers

<table>
<thead>
<tr>
<th>Peer IP Addr</th>
<th>Interface Name</th>
<th>Version</th>
<th>Last Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.5.13</td>
<td>router-2/2</td>
<td>RIPv2</td>
<td>0</td>
</tr>
<tr>
<td>10.0.6.16</td>
<td>router-2/3</td>
<td>RIPv2</td>
<td>2</td>
</tr>
<tr>
<td>10.0.9.14</td>
<td>router-2/5</td>
<td>RIPv2</td>
<td>8</td>
</tr>
<tr>
<td>10.0.10.15</td>
<td>router-2/4</td>
<td>RIPv2</td>
<td>0</td>
</tr>
</tbody>
</table>

No. of Peers: 4

---

### statistics

**Syntax**  
`statistics [ip-addr | ip-int-name]`

**Context**  
`show>router>rip`

**Description**  
Display interface level statistics for the RIP protocol.

If no IP address or interface name is specified, then all configured RIP interfaces are displayed.

If an IP address or interface name is specified, then only data regarding the specified RIP interface is displayed.

**Parameters**  
`ip-addr | ip-int-name` — Displays statistics for the specified IP interface.

**Output**  
**RIP Statistics Output** — The following table describes the output fields for RIP statistics.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learned Routes</td>
<td>The number of RIP-learned routes were exported to RIP neighbors.</td>
</tr>
<tr>
<td>Timed Out Routes</td>
<td>The number of routes that have been timed out.</td>
</tr>
<tr>
<td>Current Memory</td>
<td>The amount of memory used by this RIP router instance.</td>
</tr>
<tr>
<td>Maximum Memory</td>
<td>The amount of memory allocated for this RIP router instance.</td>
</tr>
<tr>
<td>Interface</td>
<td>Displays the name of each interface configured in RIP and associated RIP statistics.</td>
</tr>
<tr>
<td>Primary IP</td>
<td>The interface IP address.</td>
</tr>
<tr>
<td>Update Timer</td>
<td>The current setting of the RIP update timer value expressed in seconds.</td>
</tr>
<tr>
<td>Timeout Timer</td>
<td>The current RIP timeout timer value expressed in seconds.</td>
</tr>
<tr>
<td>Flush Timer</td>
<td>The number of seconds after a route has been declared invalid that it is flushed from the route database.</td>
</tr>
<tr>
<td>Updates Sent</td>
<td><strong>Total</strong> — The total number of RIP updates that were sent.</td>
</tr>
<tr>
<td></td>
<td><strong>Last 5 Min</strong> — The number of RIP updates that were sent in the last 5 minutes.</td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Triggered Updates Total</td>
<td>The total number of triggered updates sent. These updates are sent before the entire RIP routing table is sent.</td>
</tr>
<tr>
<td>Triggered Updates Last 5 Min</td>
<td>The number of triggered updates that were sent in the last 5 minutes.</td>
</tr>
<tr>
<td>Triggered Updates Last 1 Min</td>
<td>The number of triggered updates that were sent in the last 1 minute.</td>
</tr>
<tr>
<td>Bad Packets Received Total</td>
<td>The total number of RIP updates received on this interface that were discarded as invalid.</td>
</tr>
<tr>
<td>Bad Packets Received Last 5 Min</td>
<td>The number of RIP updates received on this interface that were discarded as invalid in the last 5 minutes.</td>
</tr>
<tr>
<td>Bad Packets Received Last 1 Min</td>
<td>The number of RIP updates received on this interface that were discarded as invalid in the last 1 minute.</td>
</tr>
<tr>
<td>RIPv1 Updates Received Total</td>
<td>The total number of RIPv1 updates received.</td>
</tr>
<tr>
<td>RIPv1 Updates Received Last 5 Min</td>
<td>The number of RIPv1 updates received in the last 5 minutes.</td>
</tr>
<tr>
<td>RIPv1 Updates Received Last 1 Min</td>
<td>The number of RIPv1 updates received in the last 1 minute.</td>
</tr>
<tr>
<td>RIPv1 Updates Ignored Total</td>
<td>The total number of RIPv1 updates ignored.</td>
</tr>
<tr>
<td>RIPv1 Updates Ignored Last 5 Min</td>
<td>The number of RIPv1 updates ignored in the last 5 minutes.</td>
</tr>
<tr>
<td>RIPv1 Updates Ignored Last 1 Min</td>
<td>The number of RIPv1 updates ignored in the last 1 minute.</td>
</tr>
<tr>
<td>RIPv1 Bad Routes Total</td>
<td>The total number of bad routes received from the peer.</td>
</tr>
<tr>
<td>RIPv1 Bad Routes Last 5 Min</td>
<td>The number of bad routes received from the peer in the last 5 minutes.</td>
</tr>
<tr>
<td>RIPv1 Bad Routes Last 1 Min</td>
<td>The number of bad routes received from the peer in the last 1 minute.</td>
</tr>
<tr>
<td>RIPv1 Requests Received Total</td>
<td>The total number of times the router received RIPv1 route requests from other routers.</td>
</tr>
<tr>
<td>RIPv1 Requests Received Last 5 Min</td>
<td>The number of times the router received RIPv1 route requests from other routers in the last 5 minutes.</td>
</tr>
</tbody>
</table>
### Label Description (Continued)

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RIPv1 Requests Ignored</strong></td>
<td>Last 1 Min – The number of times the router received RIPv1 route requests from other routers in the last 1 minute.</td>
</tr>
<tr>
<td></td>
<td>Total – The total number of times the router ignored RIPv1 route requests from other routers.</td>
</tr>
<tr>
<td></td>
<td>Last 5 Min – The number of times the router ignored RIPv1 route requests from other routers in the last 5 minutes.</td>
</tr>
<tr>
<td></td>
<td>Last 1 Min – The number of times the router ignored RIPv1 route requests from other routers in the last 1 minute.</td>
</tr>
<tr>
<td><strong>RIPv2 Updates Received</strong></td>
<td>Total – The total number of RIPv2 updates received.</td>
</tr>
<tr>
<td></td>
<td>Last 5 Min – The number of RIPv2 updates received in the last 5 minutes.</td>
</tr>
<tr>
<td></td>
<td>Last 1 Min – The number of RIPv2 updates received in the last minute.</td>
</tr>
<tr>
<td><strong>RIPv2 Updates Ignored</strong></td>
<td>Total – The total number of RIPv2 updates ignored.</td>
</tr>
<tr>
<td></td>
<td>Last 5 Min – The number of RIPv2 updates ignored in the last 5 minutes.</td>
</tr>
<tr>
<td></td>
<td>Last 1 Min – The number of RIPv2 updates ignored in the last minute.</td>
</tr>
<tr>
<td><strong>RIPv2 Bad Routes</strong></td>
<td>Total – The total number of RIPv2 bad routes received from the peer.</td>
</tr>
<tr>
<td></td>
<td>Last 5 Min – The number of RIPv2 bad routes received from the peer in the last 5 minutes.</td>
</tr>
<tr>
<td></td>
<td>Last 1 Min – The number of RIPv2 bad routes received from the peer in the last minute.</td>
</tr>
<tr>
<td><strong>RIPv2 Requests Received</strong></td>
<td>Total – The total number of times the router received RIPv2 route requests from other routers.</td>
</tr>
<tr>
<td></td>
<td>Last 5 Min – The number of times the router received RIPv2 route requests from other routers in the last 5 minutes.</td>
</tr>
<tr>
<td></td>
<td>Last 1 Min – The number of times the router received RIPv2 route requests from other routers in the last minute.</td>
</tr>
<tr>
<td><strong>RIPv2 Requests Ignored</strong></td>
<td>Total – The total number of times the router ignored RIPv2 route requests from other routers.</td>
</tr>
<tr>
<td></td>
<td>Last 5 Min – The number of times the router ignored RIPv2 route requests from other routers in the last 5 minutes.</td>
</tr>
</tbody>
</table>
Sample Output

A:ALA-A# show router rip statistics

RIP Statistics

Learned Routes : 0                  Timed Out Routes : 0
Current Memory : 120624             Maximum Memory : 262144

Interface "to-web"

Primary IP : 10.1.1.3               Update Timer : 30
Timeout Timer : 180                Flush Timer : 120

Counter Total Last 5 Min Last 1 Min
Updates Sent 0 0 0
Triggered Updates 0 0 0
Bad Packets Received 0 0 0
RIPv1 Updates Received 0 0 0
RIPv1 Updates Ignored 0 0 0
RIPv1 Bad Routes 0 0 0
RIPv1 Requests Received 0 0 0
RIPv1 Requests Ignored 0 0 0
RIPv2 Updates Received 0 0 0
RIPv2 Updates Ignored 0 0 0
RIPv2 Bad Routes 0 0 0
RIPv2 Requests Received 0 0 0
RIPv2 Requests Ignored 0 0 0
Authentication Errors 0 0 0

A:ALA-A#
Clear Commands

database

Syntax  database
Context  clear>router>rip
Description  Flush all routes in the RIP database.

statistics

Syntax  statistics [neighbor ip-int-name | ip-address]
Context  clear>router>rip
Description  Clears statistics for RIP neighbors.
Parameters  neighbor ip-int-name | ip-address — Clears the statistics for the specified RIP interface.
                Default  clears statistics for all RIP interfaces
Debug RIP Commands

**auth**

**Syntax**

```
[no] auth [neighbor ip-int-name | ip-addr]
```

**Context**

`debug>router>rip`

**Description**

This command enables debugging for RIP authentication.

**Parameters**

`neighbor ip-addr | ip-int-name` — Debugs the RIP authentication for the neighbor IP address or interface.

**error**

**Syntax**

```
[no] error [neighbor ip-int-name | ip-addr]
```

**Context**

`debug>router>rip`

**Description**

This command enables debugging for RIP errors.

**Parameters**

`neighbor ip-addr | ip-int-name` — Debugs the RIP errors sent on the neighbor IP address or interface.

**events**

**Syntax**

```
[no] events [neighbor ip-int-name | ip-addr]
```

**Context**

`debug>router>rip`

**Description**

This command enables debugging for RIP events.

**Parameters**

`neighbor ip-addr | ip-int-name` — Debugs the RIP events sent on the neighbor IP address or interface.

**holddown**

**Syntax**

```
[no] holddown [neighbor ip-int-name | ip-addr]
```

**Context**

`debug>router>rip`

**Description**

This command enables debugging for RIP holddowns.

**Parameters**

`neighbor ip-addr | ip-int-name` — Debugs the RIP holddowns sent on the neighbor IP address or interface.
packets

Syntax  
[no] packets [neighbor ip-int-name | ip-addr]

Context  
debug>router>rip

Description  
This command enables debugging for RIP packets.

Parameters  
neighbor ip-addr | ip-int-name — Debugs the RIP packets sent on the neighbor IP address or interface.

request

Syntax  
[no] request [neighbor ip-int-name | ip-addr]

Context  
debug>router>rip

Description  
This command enables debugging for RIP requests.

Parameters  
neighbor ip-addr | ip-int-name — Debugs the RIP requests sent on the neighbor IP address or interface.

trigger

Syntax  
[no] trigger [neighbor ip-int-name | ip-addr]

Context  
debug>router>rip

Description  
This command enables debugging for RIP trigger updates.

Parameters  
neighbor ip-addr | ip-int-name — Debugs the RIP updates sent on the neighbor IP address or interface.

updates

Syntax  
[no] updates [neighbor ip-int-name | ip-addr]

Context  
debug>router>rip

Description  
This command enables debugging for RIP updates.

Parameters  
neighbor ip-addr | ip-int-name — Debugs the RIP updates sent on the neighbor IP address or interface.
In This Chapter

This chapter provides information about configuring the Open Shortest Path First (OSPF) protocol.

Topics in this chapter include:

- Configuring OSPF on page 286
  - OSPF Areas on page 287
    - Backbone Area on page 287
    - Stub Area on page 288
    - Not-So-Stubby Area on page 289
  - OSPF Super Backbone on page 290
  - Virtual Links on page 296
  - Neighbors and Adjacencies on page 297
  - Link-State Advertisements on page 298
  - Metrics on page 298
  - Authentication on page 299
  - IP Subnets on page 300
  - Preconfiguration Recommendations on page 300
- OSPF Configuration Process Overview on page 311
- Configuration Notes on page 312
OSPF (Open Shortest Path First) is a hierarchical link state protocol. OSPF is an interior gateway protocol (IGP) used within large autonomous systems (ASs). OSPF routers exchange state, cost, and other relevant interface information with neighbors. The information exchange enables all participating routers to establish a network topology map. Each router applies the Dijkstra algorithm to calculate the shortest path to each destination in the network. The resulting OSPF forwarding table is submitted to the routing table manager to calculate the routing table.

When a router is started with OSPF configured, OSPF, along with the routing-protocol data structures, is initialized and waits for indications from lower-layer protocols that its interfaces are functional. Alcatel-Lucent’s implementation of OSPF conforms to OSPF Version 2 specifications presented in RFC 2328, *OSPF Version 2*. Routers running OSPF can be enabled with minimal configuration. All default and command parameters can be modified.

Key OSPF features are:

- Backbone areas
- Stub areas
- Not-So-Stubby areas (NSSAs)
- Virtual links
- Authentication
- Route redistribution
- Routing interface parameters
- OSPF-TE extensions (Alcatel-Lucent’s implementation allows MPLS fast reroute)
**OSPF Areas**

The hierarchical design of OSPF allows a collection of networks to be grouped into a logical area. An area’s topology is concealed from the rest of the AS which significantly reduces OSPF protocol traffic. With the proper network design and area route aggregation, the size of the route-table can be drastically reduced which results in decreased OSPF route calculation time and topological database size.

Routing in the AS takes place on two levels, depending on whether the source and destination of a packet reside in the same area (intra-area routing) or different areas (inter-area routing). In intra-area routing, the packet is routed solely on information obtained within the area; no routing information obtained from outside the area is used.

Routers that belong to more than one area are called area border routers (ABRs). An ABR maintains a separate topological database for each area it is connected to. Every router that belongs to the same area has an identical topological database for that area.

---

**Backbone Area**

The OSPF backbone area, area 0.0.0.0, must be contiguous and all other areas must be connected to the backbone area. The backbone distributes routing information between areas. If it is not practical to connect an area to the backbone (see area 0.0.0.5 in Figure 7) then the ABRs (such as routers Y and Z) must be connected via a virtual link. The two ABRs form a point-to-point-like adjacency across the transit area (see area 0.0.0.4).
Stub Area

A stub area is a designated area that does not allow external route advertisements. Routers in a stub area do not maintain external routes. A single default route to an ABR replaces all external routes. This OSPF implementation supports the optional summary route (type-3) advertisement suppression from other areas into a stub area. This feature further reduces topological database sizes and OSPF protocol traffic, memory usage, and CPU route calculation time.

In Figure 7, areas 0.0.0.1, 0.0.0.2 and 0.0.0.5 could be configured as stub areas. A stub area cannot be designated as the transit area of a virtual link and a stub area cannot contain an AS boundary router. An AS boundary router exchanges routing information with routers in other ASs.
Not-So-Stubby Area

Another OSPF area type is called a Not-So-Stubby area (NSSA). NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. External routes learned by OSPF routers in the NSSA area are advertised as type-7 LSAs within the NSSA area and are translated by ABRs into type-5 external route advertisements for distribution into other areas of the OSPF domain. An NSSA area cannot be designated as the transit area of a virtual link.

In Figure 7, area 0.0.0.3 could be configured as a NSSA area.
OSPF Super Backbone

The 77x0 PE routers have implemented a version of the BGP/OSPF interaction procedures as defined in RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*. Features included in this RFC includes:

- Loop prevention
- Handling LSAs received from the CE
- Sham links
- Managing VPN-IPv4 routes received by BGP

VPRN routes can be distributed among the PE routers by BGP. If the PE uses OSPF to distribute routes to the CE router, the standard procedures governing BGP/OSPF interactions causes routes from one site to be delivered to another in type 5 LSAs, as AS-external routes.

The MPLS VPN super backbone behaves like an additional layer of hierarchy in OSPF. The PE-routers that connect the respective OSPF areas to the super backbone function as OSPF Area Border Routers (ABR) in the OSPF areas to which they are attached. In order to achieve full compatibility, they can also behave as AS Boundary Routers (ASBR) in non-stub areas.

The PE-routers insert inter-area routes from other areas into the area in which the CE-router is present. The CE-routers are not involved at any level nor are they aware of the super backbone or of other OSPF areas present beyond the MPLS VPN super backbone.

The CE always assumes the PE is an ABR:

- If the CE is in the backbone then the CE router assumes that the PE is an ABR linking one or more areas to the backbone.
- If the CE in not in the backbone then the CE believes that the backbone is on the other side of the PE.
- As such the super backbone looks like another area to the CE.
In Figure 8, the PEs are connected to the MPLS-VPN super backbone. In order to be able to distinguish if two OSPF instances are in fact the same and require Type 3 LSAs to be generated or are two separate routing instances where type 5 external LSAs need to be generated the concept of a domain-id is introduced.

The domain ID is carried with the MP-BGP update and indicates the source OSPF Domain. When the routes are being redistributed into the same OSPF Domain, the concepts of super backbone described above apply and Type 3 LSAs should be generated. If the OSPF domain does not match, then the route type will be external.

Configuring the super backbone (not the sham links) makes all destinations learned by PEs with matching domain IDs inter-area routes.

When configuring sham links, these links become intra-area routes if they are present in the same area.
Sham Links

Figure 9: Sham Links

Figure 9 displays the red link between CE-3 and CE-4 could be a low speed OC-3/STM-1 link but because it establishes a intra-area route connection between the CE-3 and CE-4 the potentially high-speed PE-1 to PE-2 connection will not be utilized. Even with a super backbone configuration it is regarded as a inter-area connection.

The establishment of the (green) sham-link is also constructed as an intra-area link between PE routers, a normal OSPF adjacency is formed and the link-state database is exchanged across the MPLS-VPRN. As a result, the desired intra-area connectivity is created, at this time the cost of the green and red links can be managed such that the red link becomes a standby link only in case the VPN fails.

As the shamlink forms an adjacency over the MPLS-VPRN backbone network, be aware that when protocol-protection is enabled in the config>sys>security>cpu-protection>protocol-protection context, the operator must explicit allow the OSPF packets to be received over the backbone network. This performed using the allow-sham-links parameter of the protocol-protection command.
Implementing the OSPF Super Backbone

With the OSPF super backbone architecture, the continuity of OSPF routing is preserved:

- The OSPF intra-area LSAs (type-1 and type-2) advertised by the CE are inserted into the MPLS-VPRN super backbone by redistributing the OSPF route into MP-BGP by the PE adjacent to the CE.
- The MP-BGP route is propagated to other PE-routers and inserted as an OSPF route into other OSPF areas. Considering the PEs across the super backbone always act as ABRs, they will generate inter area route OSPF summary LSAs, Type 3.
- The inter-area route can now be propagated into other OSPF areas by other customer-owned ABRs within the customer site.
- Customer Area 0 (backbone) routes when carried across the MPLS-VPRN using MPBGP will appear as Type 3 LSAs even if the customer area remains area 0 (backbone).

A BGP extended community (OSPF domain ID) provides the source domain of the route. This domain ID is not carried by OSPF but carried by MP-BGP as an extended community attribute.

If the configured extended community value matches the receiving OSPF domain, then the OSPF super backbone is implemented.

From a BGP perspective, the cost is copied into the MED attribute.

Loop Avoidance

If a route sent from a PE router to a CE router could then be received by another PE router from one of its own CE routers then it is possible for routing loops to occur. RFC 4577 specifies several methods of loop avoidance.

DN-BIT

When a Type 3 LSA is sent from a PE router to a CE router, the DN bit in the LSA options field is set. This is used to ensure that if any CE router sends this Type 3 LSA to a PE router, the PE router will not redistribute it further.

When a PE router needs to distribute to a CE router a route that comes from a site outside the latter's OSPF domain, the PE router presents itself as an ASBR (Autonomous System Border Router), and distributes the route in a type 5 LSA. The DN bit MUST be set in these LSAs to ensure that they will be ignored by any other PE routers that receive them.

DN-BIT loop avoidance is also supported.
Configuring OSPF

Route Tag

If a particular VRF in a PE is associated with an instance of OSPF, then by default it is configured with a special OSPF route tag value called the VPN route tag. This route tag is included in the Type 5 LSAs that the PE originates and sends to any of the attached CEs. The configuration and inclusion of the VPN Route Tag is required for backward compatibility with deployed implementations that do not set the DN bit in Type 5 LSAs.

Sham Links

A sham link is only required if a backdoor link (shown as the red link in Figure 9) is present, otherwise configuring an OSPF super backbone will probably suffice.
**OSPFv3 Graceful Restart Helper**

This feature extends the Graceful Restart helper function supported under other protocols to OSPFv3.

The primary difference between graceful restart helper for OSPFv2 and OSPFv3 is in OSPFv3 a different grace-LSA format is used.

As the SR-OS platforms can support a fully non-stop routing model for control plane high availability the SR-OS node has no need for graceful restart as defined by the IETF in various RFCs for each routing protocol. However, since the 7x50 does need to co-exist in multi-vendor networks and other routers do not always support a true non-stop routing model with stateful failover between routing control planes, there is a need to support a Graceful Restart Helper function.

Graceful restart helper mode allows the SROS based system to provide other routers which have requested it, a grace period, during which the SR-OS systems will continue to use routes authored by or transiting the router requesting the grace period. This is typically used when another router is rebooting the control plane but the forwarding plane is expected to continue to forward traffic based on the previously available FIB.
Virtual Links

The backbone area in an OSPF AS must be contiguous and all other areas must be connected to the backbone area. Sometimes, this is not possible. You can use virtual links to connect to the backbone through a non-backbone area.

Figure 7 depicts routers Y and Z as the start and end points of the virtual link while area 0.0.0.4 is the transit area. In order to configure virtual links, the router must be an ABR. Virtual links are identified by the router ID of the other endpoint, another ABR. These two endpoint routers must be attached to a common area, called the transit area. The area through which you configure the virtual link must have full routing information.

Transit areas pass traffic from an area adjacent to the backbone or to another area. The traffic does not originate in, nor is it destined for, the transit area. The transit area cannot be a stub area or a NSSA area.

Virtual links are part of the backbone, and behave as if they were unnumbered point-to-point networks between the two routers. A virtual link uses the intra-area routing of its transit area to forward packets. Virtual links are brought up and down through the building of the shortest-path trees for the transit area.
Neighbors and Adjacencies

A router uses the OSPF Hello protocol to discover neighbors. A neighbor is a router configured with an interface to a common network. The router sends hello packets to a multicast address and receives hello packets in return.

In broadcast networks, a designated router and a backup designated router are elected. The designated router is responsible for sending link-state advertisements (LSAs) describing the network, which reduces the amount of network traffic.

The routers attempt to form adjacencies. An adjacency is a relationship formed between a router and the designated or backup designated router. For point-to-point networks, no designated or backup designated router is elected. An adjacency must be formed with the neighbor.

To significantly improve adjacency forming and network convergence, a network should be configured as point-to-point if only two routers are connected, even if the network is a broadcast media such as Ethernet.

When the link-state databases of two neighbors are synchronized, the routers are considered to be fully adjacent. When adjacencies are established, pairs of adjacent routers synchronize their topological databases. Not every neighboring router forms an adjacency. Routing protocol updates are only sent to and received from adjacencies. Routers that do not become fully adjacent remain in the two-way neighbor state.
Link-State Advertisements

Link-state advertisements (LSAs) describe the state of a router or network, including router interfaces and adjacency states. Each LSA is flooded throughout an area. The collection of LSAs from all routers and networks form the protocol's topological database.

The distribution of topology database updates take place along adjacencies. A router sends LSAs to advertise its state according to the configured interval and when the router's state changes. These packets include information about the router's adjacencies, which allows detection of non-operational routers.

When a router discovers a routing table change or detects a change in the network, link state information is advertised to other routers to maintain identical routing tables. Router adjacencies are reflected in the contents of its link state advertisements. The relationship between adjacencies and the link states allow the protocol to detect non-operating routers. Link state advertisements flood the area. The flooding mechanism ensures that all routers in an area have the same topological database. The database consists of the collection of LSAs received from each router belonging to the area.

OSPF sends only the part that has changed and only when a change has taken place. From the topological database, each router constructs a tree of shortest paths with itself as root. OSPF distributes routing information between routers belonging to a single AS.

Metrics

In OSPF, all interfaces have a cost value or routing metric used in the OSPF link-state calculation. A metric value is configured based on hop count, bandwidth, or other parameters, to compare different paths through an AS. OSPF uses cost values to determine the best path to a particular destination: the lower the cost value, the more likely the interface will be used to forward data traffic.

Costs are also associated with externally derived routing data, such as those routes learned from the Exterior Gateway Protocol (EGP), like BGP, and is passed transparently throughout the AS. This data is kept separate from the OSPF protocol's link state data. Each external route can be tagged by the advertising router, enabling the passing of additional information between routers on the boundaries of the AS.
Authentication

All OSPF protocol exchanges can be authenticated. This means that only trusted routers can participate in autonomous system routing. Alcatel-Lucent’s implementation of OSPF supports plain text and Message Digest 5 (MD5) authentication (also called simple password).

MD5 allows an authentication key to be configured per network. Routers in the same routing domain must be configured with the same key. When the MD5 hashing algorithm is used for authentication, MD5 is used to verify data integrity by creating a 128-bit message digest from the data input. It is unique to that data. Alcatel-Lucent’s implementation of MD5 allows the migration of an MD5 key by using a key ID for each unique key.

By default, authentication is not enabled on an interface.
IP Subnets

OSPF enables the flexible configuration of IP subnets. Each distributed OSPF route has a destination and mask. A network mask is a 32-bit number that indicates the range of IP addresses residing on a single IP network/subnet. This specification displays network masks as hexadecimal numbers; for example, the network mask for a class C IP network is displayed as 0xffffff00. Such a mask is often displayed as 255.255.255.0.

Two different subnets with same IP network number have different masks, called variable length subnets. A packet is routed to the longest or most specific match. Host routes are considered to be subnets whose masks are all ones (0xffffffff).

Preconfiguration Recommendations

Prior to configuring OSPF, the router ID must be available. The router ID is a 32-bit number assigned to each router running OSPF. This number uniquely identifies the router within an AS. OSPF routers use the router IDs of the neighbor routers to establish adjacencies. Neighbor IDs are learned when Hello packets are received from the neighbor.

Before configuring OSPF parameters, ensure that the router ID is derived by one of the following methods:

- Define the value in the config>router router-id context.
- Define the system interface in the config>router>interface ip-int-name context (used if the router ID is not specified in the config>router router-id context).

  A system interface must have an IP address with a 32-bit subnet mask. The system interface is used as the router identifier by higher-level protocols such as OSPF and IS-IS. The system interface is assigned during the primary router configuration process when the interface is created in the logical IP interface context.

- If you do not specify a router ID, then the last four bytes of the MAC address are used.

NOTE: On the BGP protocol level, a BGP router ID can be defined in the config>router>bgp router-id context and is only used within BGP.
Multiple OSPF Instances

The main route table manager (RTM) can create multiple instances of OSPF by extending the current creation of an instance. A given interface can only be a member of a single OSPF instance. When an interface is configured in a given domain and needs to be moved to another domain, the interface must first be removed from the old instance and re-created in the new instance.

Route Export Policies for OSPF

Route policies allow specification of the source OSPF process ID in the `from` and `to` parameters in the `config>router>policy-options>policy-statement>entry>from` context, for example `from protocol ospf instance-id`.

If an `instance-id` is specified, only routes installed by that instance are picked up for announcement. If no `instance-id` is specified, then only routes installed by the base instance is will be announced. The `all` keyword announces routes installed by all instances of OSPF.

When announcing internal (intra/inter-area) OSPF routes from another process, the default type should be type-1, and metric set to the route metric in RTM. For AS-external routes, by default the route type (type-1/2) should be preserved in the originated LSA, and metric set to the route metric in RTM. By default, the tag value should be preserved when an external OSPF route is announced by another process. All these can be changed with explicit action statements.

Export policy should allow a match criteria based on the OSPF route hierarchy, e.g. only intra-area, only inter-area, only external, only internal (intra/inter-area). There must also be a possibility to filter based on existing tag values.
Preventing Route Redistribution Loops

The legacy method for this was to assign a tag value to each OSPF process and mark each external route originated within that domain with that value. However, since the tag value must be preserved throughout different OSPF domains, this only catches loops that go back to the originating domain and not where looping occurs in a remote set of domains. To prevent this type of loop, the route propagation information in the LSA must be accumulative. The following method has been implemented:

- The OSPF tag field in the AS-external LSAs is treated as a bit mask, rather than a scalar value. In other words, each bit in the tag value can be independently checked, set or reset as part of the routing policy.

- When a set of OSPF domains are provisioned in a network, each domain is assigned a specific bit value in the 32-bit tag mask. When an external route is originated by an ASBR using an internal OSPF route in a given domain, a corresponding bit is set in the AS-external LSA. As the route gets redistributed from one domain to another, more bits are set in the tag mask, each corresponding to the OSPF domain the route visited. Route redistribution looping is prevented by checking the corresponding bit as part of the export policy--if the bit corresponding to the announcing OSPF process is already set, the route is not exported there.

From the CLI perspective, this involves adding a set of `from tag` and `action tag` commands that allow for bit operations.
IP Fast-reroute (IP FRR) For OSPF and IS-IS Prefixes

This feature provides for the use of the Loop-Free Alternate (LFA) backup next-hop for forwarding in-transit and CPM generated IP packets when the primary next-hop is not available. This means that a node resumes forwarding IP packets to a destination prefix without waiting for the routing convergence.

When any of the following events occurs, IGP instructs in the fast path the IOM to enable the LFA backup next-hop:

- OSPF/IS-IS interface goes operationally down: physical or local admin shutdown.
- Timeout of a BFD session to a next-hop when BFD is enabled on the OSPF/IS-IS interface.

IP FRR is supported on IPv4 and IPv6 OSPF/IS-IS prefixes forwarded in the base router instance to a network IP interface or to an IES SAP interface or spoke interface. It is also supported for VPRN VPN-IPv4 OSPF prefixes and VPN-IPv6 OSPF prefixes forwarded to a VPRN SAP interface or spoke interface.

IP FRR also provides a LFA backup next-hop for the destination prefix of a GRE tunnel used in an SDP or in VPRN auto-bind.

The LFA next-hop pre-computation by IGP is described in RFC 5286 – “Basic Specification for IP Fast Reroute: Loop-Free Alternates”.

IP FRR Configuration

The user first enables Loop-Free Alternate (LFA) computation by SPF under the IS-IS routing protocol level or under the OSPF routing protocol instance level:

```
config>router>isis>loopfree-alternate
config>router>ospf>loopfree-alternate
config>service>vprn>ospf>loopfree-alternate
```

The above commands instruct the IGP SPF to attempt to pre-compute both a primary next-hop and an LFA next-hop for every learned prefix. When found, the LFA next-hop is populated into the RTM along with the primary next-hop for the prefix.

Next the user enables IP FRR to cause RTM to download to IOM a LFA next-hop, when found by SPF, in addition to the primary next-hop for each prefix in the FIB.

```
config>router>ip-fast-reroute
```
Reducing the Scope of the LFA Calculation by SPF

The user can instruct IGP to not include all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

```
config>router>isis>level>loopfree-alternate-exclude
config>router>ospf>area>loopfree-alternate-exclude
```

The user can also exclude a specific IP interface from being included in the LFA SPF computation by IS-IS or OSPF:

```
config>router>isis>interface>loopfree-alternate-exclude
config>router>ospf>area>interface>loopfree-alternate-exclude
```

Note that when an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When the user excludes an interface from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

Finally, the user can apply the same above commands for an OSPF instance within a VPRN service:

```
config>service>vprn>ospf>area>loopfree-alternate-exclude
config>service>vprn>ospf>area>interface>loopfree-alternate-exclude
```

ECMP Considerations

Whenever the SPF computation determined there is more than one primary next-hop for a prefix, it will not program any LFA next-hop in RTM. Thus, IP prefixes will resolve to the multiple primary next-hops in this case which provides the required protection.
IP FRR and RSVP Shortcut (IGP Shortcut)

When both IGP shortcut and LFA are enabled in IS-IS or OSPF, and IP FRR is also enabled, then the following additional IP FRR capabilities are supported:

- A prefix which is resolved to a direct primary next-hop can be backed up by a tunneled LFA next-hop.
- A prefix which is resolved to a tunneled primary next-hop will not have an LFA next-hop. It will rely on RSVP FRR for protection.

The LFA SPF is extended to use IGP shortcuts as LFA next-hops as explained in OSPF and IS-IS Support for Loop-Free Alternate Calculation on page 305.

IP FRR and BGP Next-Hop Resolution

An LFA backup next-hop will be able to protect the primary next-hop to reach a prefix advertised by a BGP neighbor. The BGP next-hop will thus remain up when the FIB switches from the primary IGP next-hop to the LFA IGP next-hop.

OSPF and IS-IS Support for Loop-Free Alternate Calculation

SPF computation in IS-IS and OSPF is enhanced to compute LFA alternate routes for each learned prefix and populate it in RTM.

Figure 10 illustrates a simple network topology with point-to-point (P2P) interfaces and highlights three routes to reach router R5 from router R1.
Figure 10: Example Topology with Primary and LFA Routes

The primary route is via R3. The LFA route via R2 has two equal cost paths to reach R5. The path by way of R3 protects against failure of link R1-R3. This route is computed by R1 by checking that the cost for R2 to reach R5 by way of R3 is lower than the cost by way of routes R1 and R3. This condition is referred to as the “loop-free criterion”.

The path by way of R2 and R4 can be used to protect against the failure of router R3. However, with the link R2-R3 metric set to 5, R2 sees the same cost to forward a packet to R5 by way of R3 and R4. Thus R1 cannot guarantee that enabling the LFA next-hop R2 will protect against R3 node failure. This means that the LFA next-hop R2 provides link-protection only for prefix R5. If the metric of link R2-R3 is changed to 8, then the LFA next-hop R2 provides node protection since a packet to R5 will always go over R4. In other words it is required that R2 becomes loop-free with respect to both the source node R1 and the protected node R3.
Consider now the case where the primary next-hop uses a broadcast interface as illustrated in Figure 11.

![Figure 11: Example Topology with Broadcast Interfaces](image)

**Figure 11: Example Topology with Broadcast Interfaces**

In order for next-hop R2 to be a link-protect LFA for route R5 from R1, it must be loop-free with respect to the R1-R3 link Pseudo-Node (PN). However, since R2 has also a link to that PN, its cost to reach R5 by way of the PN, or router R4 are the same. Thus R1 cannot guarantee that enabling the LFA next-hop R2 will protect against a failure impacting link R1-PN since this may cause the entire subnet represented by the PN to go down. If the metric of link R2-PN is changed to 8, then R2 next-hop will be an LFA providing link protection.
The following are the detailed equations for this criterion as provided in RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*:

- **Rule 1**: Link-protect LFA backup next-hop (primary next-hop R1-R3 is a P2P interface):
  \[ \text{Distance}_{\text{opt}}(R2, R5) < \text{Distance}_{\text{opt}}(R2, R1) + \text{Distance}_{\text{opt}}(R1, R5) \]
  and,
  \[ \text{Distance}_{\text{opt}}(R2, R5) \geq \text{Distance}_{\text{opt}}(R2, R3) + \text{Distance}_{\text{opt}}(R3, R5) \]

- **Rule 2**: Node-protect LFA backup next-hop (primary next-hop R1-R3 is a P2P interface):
  \[ \text{Distance}_{\text{opt}}(R2, R5) < \text{Distance}_{\text{opt}}(R2, R1) + \text{Distance}_{\text{opt}}(R1, R5) \]
  and,
  \[ \text{Distance}_{\text{opt}}(R2, R5) < \text{Distance}_{\text{opt}}(R2, R3) + \text{Distance}_{\text{opt}}(R3, R5) \]

- **Rule 3**: Link-protect LFA backup next-hop (primary next-hop R1-R3 is a broadcast interface):
  \[ \text{Distance}_{\text{opt}}(R2, R5) < \text{Distance}_{\text{opt}}(R2, R1) + \text{Distance}_{\text{opt}}(R1, R5) \]
  and,
  \[ \text{Distance}_{\text{opt}}(R2, R5) < \text{Distance}_{\text{opt}}(R2, PN) + \text{Distance}_{\text{opt}}(PN, R5) \]
  where; PN stands for the R1-R3 link Pseudo-Node.

For the case of P2P interface, if SPF finds multiple LFA next-hops for a given primary next-hop, it follows the following selection algorithm:

A) It will pick the node-protect type in favor of the link-protect type.

B) If there is more than one LFA next-hop within the selected type, then it will pick one based on the least cost.

C) If more than one LFA next-hop with the same cost results from step (b), then SPF will select the first one. This is not a deterministic selection and will vary following each SPF calculation.

For the case of a broadcast interface, a node-protect LFA is not necessarily a link protect LFA if the path to the LFA next-hop goes over the same PN as the primary next-hop. Similarly, a link protect LFA may not guarantee link protection if it goes over the same PN as the primary next-hop. The selection algorithm when SPF finds multiple LFA next-hops for a given primary next-hop is modified as follows:

A) The algorithm splits the LFA next-hops into two sets:
   - The first set consists of LFA next-hops which *do not* go over the PN used by primary next-hop.
   - The second set consists of LFA next-hops which *do* go over the PN used by the primary next-hop.

B) If there is more than one LFA next-hop in the first set, it will pick the node-protect type in favor of the link-protect type.
C) If there is more than one LFA next-hop within the selected type, then it will pick one based on the least cost.

D) If more than one LFA next-hop with equal cost results from Step C, SPF will select the first one from the remaining set. This is not a deterministic selection and will vary following each SPF calculation.

E) If no LFA next-hop results from Step D, SPF will rerun Steps B-D using the second set.

Note this algorithm is more flexible than strictly applying Rule 3 above; i.e., the link protect rule in the presence of a PN and specified in RFC 5286. A node-protect LFA which does not avoid the PN; i.e., does not guarantee link protection, can still be selected as a last resort. The same thing, a link-protect LFA which does not avoid the PN may still be selected as a last resort.

Both the computed primary next-hop and LFA next-hop for a given prefix are programmed into RTM.

Loop-Free Alternate Calculation in the Presence of IGP shortcuts

In order to expand the coverage of the LFA backup protection in a network, RSVP LSP based IGP shortcuts can be placed selectively in parts of the network and be used as an LFA backup next-hop.

When IGP shortcut is enabled in IS-IS or OSPF on a given node, all RSVP LSP originating on this node and with a destination address matching the router-id of any other node in the network are included in the main SPF by default.

In order to limit the time it takes to compute the LFA SPF, the user must explicitly enable the use of an IGP shortcut as LFA backup next-hop using one of a couple of new optional argument for the existing LSP level IGP shortcut command:

```
config>router>mpls>lsp>igp-shortcut [lfa-protect | lfa-only]
```

The `lfa-protect` option allows an LSP to be included in both the main SPF and the LFA SPFs. For a given prefix, the LSP can be used either as a primary next-hop or as an LFA next-hop but not both. If the main SPF computation selected a tunneled primary next-hop for a prefix, the LFA SPF will not select an LFA next-hop for this prefix and the protection of this prefix will rely on the RSVP LSP FRR protection. If the main SPF computation selected a direct primary next-hop, then the LFA SPF will select an LFA next-hop for this prefix but will prefer a direct LFA next-hop over a tunneled LFA next-hop.

The `lfa-only` option allows an LSP to be included in the LFA SPFs only such that the introduction of IGP shortcuts does not impact the main SPF decision. For a given prefix, the main SPF always selects a direct primary next-hop. The LFA SPF will select a an LFA next-hop for this prefix but will prefer a direct LFA next-hop over a tunneled LFA next-hop.
Thus the selection algorithm in Section 1.3 when SPF finds multiple LFA next-hops for a given primary next-hop is modified as follows:

A) The algorithm splits the LFA next-hops into two sets:
   - the first set consists of direct LFA next-hops
   - the second set consists of tunneled LFA next-hops after excluding the LSPs which use the same outgoing interface as the primary next-hop.

B) The algorithms continues with first set if not empty, otherwise it continues with second set.

C) If the second set is used, the algorithm selects the tunneled LFA next-hop which endpoint corresponds to the node advertising the prefix.
   - If more than one tunneled next-hop exists, it selects the one with the lowest LSP metric.
   - If still more than one tunneled next-hop exists, it selects the one with the lowest tunnel-id.
   - If none is available, it continues with rest of the tunneled LFAs in second set.

D) Within the selected set, the algorithm splits the LFA next-hops into two sets:
   - The first set consists of LFA next-hops which do not go over the PN used by primary next-hop.
   - The second set consists of LFA next-hops which go over the PN used by the primary next-hop.

E) If there is more than one LFA next-hop in the selected set, it will pick the node-protect type in favor of the link-protect type.

F) If there is more than one LFA next-hop within the selected type, then it will pick one based on the least total cost for the prefix. For a tunneled next-hop, it means the LSP metric plus the cost of the LSP endpoint to the destination of the prefix.

G) If there is more than one LFA next-hop within the selected type (ecmp-case) in the first set, it will select the first direct next-hop from the remaining set. This is not a deterministic selection and will vary following each SPF calculation.

H) If there is more than one LFA next-hop within the selected type (ecmp-case) in the second set, it will pick the tunneled next-hop with the lowest cost from the endpoint of the LSP to the destination prefix. If there remains more than one, it will pick the tunneled next-hop with the lowest tunnel-id.

Loop-Free Alternate Calculation for Inter-Area/inter-Level Prefixes

When SPF resolves OSPF inter-area prefixes or IS-IS inter-level prefixes, it will compute an LFA backup next-hop to the same exit area/border router as used by the primary next-hop.
OSPF Configuration Process Overview

Figure 12 displays the process to provision basic OSPF parameters.

Figure 12: OSPF Configuration and Implementation Flow
Configuration Notes

This section describes OSPF configuration caveats.

General

- Before OSPF can be configured, the router ID must be configured.
- The basic OSPF configuration includes at least one area and an associated interface.
- All default and command parameters can be modified.

OSPF Defaults

The following list summarizes the OSPF configuration defaults:

- By default, a router has no configured areas.
- An OSPF instance is created in the administratively enabled state.
Configuring OSPF with CLI

This section provides information to configure Open Shortest Path First (OSPF) using the command line interface.

Topics in this section include:

- OSPF Configuration Guidelines on page 314
- Basic OSPF Configuration on page 315
- Configuring the Router ID on page 316
- Configuring OSPF Components on page 317
  - Configuring the Router ID on page 316
  - Configuring an OSPF Area on page 318
  - Configuring a Stub Area on page 319
  - Configuring a Not-So-Stubby Area on page 320
  - Configuring a Virtual Link on page 321
  - Configuring an Interface on page 323
  - Configuring Authentication on page 325
  - Assigning a Designated Router on page 328
  - Configuring Route Summaries on page 330
  - Configuring Route Preferences on page 332
- OSPF Configuration Management Tasks on page 334
  - Modifying a Router ID on page 334
  - Deleting a Router ID on page 336
  - Modifying OSPF Parameters on page 337
OSPF Configuration Guidelines

Configuration planning is essential to organize routers, backbone, non-backbone, stub, NSSA areas, and transit links. OSPF provides essential defaults for basic protocol operability. You can configure or modify commands and parameters. OSPF is not enabled by default.

The minimal OSPF parameters which should be configured to deploy OSPF are:

- **Router ID**
  Each router running OSPF must be configured with a unique router ID. The router ID is used by both OSPF and BGP routing protocols in the routing table manager.
  When configuring a new router ID, protocols will not automatically be restarted with the new router ID. Shut down and restart the protocol to initialize the new router ID.

- **OSPF Instance**
  OSPF instances must be defined when configuring multiple instances and/or the instance being configured is not the base instance.

- **An area**
  At least one OSPF area must be created. An interface must be assigned to each OSPF area.

- **Interfaces**
  An interface is the connection between a router and one of its attached networks. An interface has state information associated with it, which is obtained from the underlying lower level protocols and the routing protocol itself. An interface to a network has associated with it a single IP address and mask (unless the network is an unnumbered point-to-point network). An interface is sometimes also referred to as a link.
Basic OSPF Configuration

This section provides information to configure OSPF as well as configuration examples of common configuration tasks.

The minimal OSPF parameters that need to be configured are:

- A router ID - If a router-id is not configured in the config>router context, the router’s system interface IP address is used.
- One or more areas.
- Interfaces (interface "system").

Following is an example of a basic OSPF configuration:

```
ALA-A>config>router>ospf# info
----------------------------------------------
  area 0.0.0.0
    interface "system"
    exit
  exit
  area 0.0.0.20
    nssa
    exit
    interface "to-104"
    priority 10
    exit
  exit
  area 0.0.1.1
  exit
----------------------------------------------
ALA-A>config>router>ospf#
```
Configuring the Router ID

The router ID uniquely identifies the router within an AS. In OSPF, routing information is exchanged between autonomous systems, groups of networks that share routing information. It can be set to be the same as the loopback (system interface) address. Subscriber services also use this address as far-end router identifiers when service distribution paths (SDPs) are created. The router ID is used by both OSPF and BGP routing protocols. A router ID can be derived by:

- Defining the value in the `config>router router-id` context.
- Defining the system interface in the `config>router>interface ip-int-name` context (used if the router ID is not specified in the `config>router router-id` context).
- Inheriting the last four bytes of the MAC address.
- On the BGP protocol level. A BGP router ID can be defined in the `config>router:bgp router-id` context and is only used within BGP.

When configuring a new router ID, protocols are not automatically restarted with the new router ID. The next time a protocol is (re)initialized the new router ID is used. An interim period of time can occur when different protocols use different router IDs. To force the new router ID, issue the `shutdown` and `no shutdown` commands for each protocol that uses the router ID or restart the entire router.

The following displays a router ID configuration example:

```
A:ALA-B>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
interface "system"
    address 10.10.10.104/32
exit
interface "to-103"
    address 10.0.0.104/24
    port 1/1/1
exit
autonomous-system 100
router-id 10.10.10.104
... #------------------------------------------
A:ALA-B>config>router#
```
Configuring OSPF Components

Use the CLI syntax displayed below for:

- Configuring OSPF Parameters on page 317
- Configuring a Stub Area on page 319
- Configuring a Not-So-Stubby Area on page 320
- Configuring a Virtual Link on page 321
- Configuring an Interface on page 323
- Configuring Authentication on page 325
- Assigning a Designated Router on page 328
- Configuring Route Summaries on page 330

Configuring OSPF Parameters

The following displays a basic OSPF configuration example:

```
A:ALA-49>config>router>ospf# info
----------------------------------------------
asbr
overload
overload-on-boot timeout 60
traffic-engineering
export "OSPF-Export"
graceful-restart
    helper-disable
exit
----------------------------------------------
A:ALA-49>config>router>ospf# ex
```
Configuring an OSPF Area

An OSPF area consists of routers configured with the same area ID. To include a router in a specific area, the common area ID must be assigned and an interface identified.

If your network consists of multiple areas you must also configure a backbone area (0.0.0.0) on at least one router. The backbone is comprised of the area border routers and other routers not included in other areas. The backbone distributes routing information between areas. The backbone is considered to be a participating area within the autonomous system. To maintain backbone connectivity, there must be at least one interface in the backbone area or have a virtual link configured to another router in the backbone area.

The minimal configuration must include an area ID and an interface. Modifying other command parameters are optional.

Use the following CLI syntax to configure an OSPF area:

CLI Syntax:  ospf ospf-instance
              area area-id
              area-range ip-prefix/mask [advertise|not-advertise]
              blackhole-aggregate

The following displays an OSPF area configuration example:

A:ALA-A>config>router>ospf# info
----------------------------------------------
area 0.0.0.0
exit
area 0.0.0.20
exit
----------------------------------------------
ALA-A>config>router>ospf#A:
Configuring a Stub Area

Configure stub areas to control external advertisements flooding and to minimize the size of the topological databases on an area’s routers. A stub area cannot also be configured as an NSSA.

By default, summary route advertisements are sent into stub areas. The no form of the summary command disables sending summary route advertisements and only the default route is advertised by the ABR. This example retains the default so the command is not entered.

If this area is configured as a transit area for a virtual link, then existing virtual links of a non-stub or NSSA area are removed when its designation is changed to NSSA or stub.

Use the following CLI syntax to configure virtual links:

**CLI Syntax:**
```
ospf
    area area-id
    stub
    default-metric metric
    summaries
```

The following displays a stub configuration example:

```
ALA-A>config>router>ospf>area# info
----------------------------------------------
...       area 0.0.0.0
          exit
          area 0.0.0.20
          stub
          exit
          exit
...  
----------------------------------------------
ALA-A>config>router>ospf#
```

The following displays a stub configuration example:

```
ALA-A>config>router>ospf>area# info
----------------------------------------------
...       area 0.0.0.0
          exit
          area 0.0.0.20
          stub
          exit
          exit
...  
----------------------------------------------
ALA-A>config>router>ospf#
```
Configuring a Not-So-Stubby Area

You must explicitly configure an area to be a Not-So-Stubby Area (NSSA) area. NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is an NSSA has the capability to flood external routes it learns throughout its area and by an area border router to the entire OSPF domain. An area cannot be both a stub area and an NSSA.

If this area is configured as a transit area for a virtual link, then existing virtual links of a non-stub or NSSA area are removed when its designation is changed to NSSA or stub.

Use the following CLI syntax to configure stub areas:

**CLI Syntax:**

```
ospf ospf-instance
area area-id
  nssa
    area-range ip-prefix/mask [advertise|not-advertise]
    originate-default-route [type-7]
    redistribute-external
    summaries
```

The following displays an NSSA configuration example:

```
A:ALA-49>config>router>ospf# info
----------------------------------------------
asbr
overload
overload-on-boot timeout 60
traffic-engineering
export "OSPF-Export"
graceful-restart
  helper-disable
exit
area 0.0.0.0
exit
area 0.0.0.20
  stub
  exit
exit
area 0.0.0.25
  nssa
  exit
exit
----------------------------------------------
A:ALA-49>config>router>ospf#
```
Configuring a Virtual Link

The backbone area (area 0.0.0.0) must be contiguous and all other areas must be connected to the backbone area. If it is not practical to connect an area to the backbone then the area border routers must be connected via a virtual link. The two area border routers will form a point-to-point-like adjacency across the transit area. A virtual link can only be configured while in the area 0.0.0.0 context.

The `router-id` parameter specified in the `virtual-link` command must be associated with the virtual neighbor, that is, enter the virtual neighbor’s router ID, not the local router ID. The transit area cannot be a stub area or an NSSA.

Use the following CLI syntax to configure stub areas:

```
CLI Syntax: ospf ospf-instance
            area area-id
                  virtual-link router-id transit-area area-id
                          authentication-key [authentication-key|hash-key]
                          [hash]
                          authentication-type [password|message-digest]
                          dead-interval seconds
                          hello-interval seconds
                          message-digest-key key-id md5 [key|hash-key]
                          [hash|hash2]
                          retransmit-interval seconds
                          transit-delay
                          no shutdown
```

The following displays a virtual link configuration example:

```
A:ALA-49>config>router>ospf# info
----------------------------------------------
 asbr
 overload
 overload-on-boot timeout 60
 traffic-engineering
 export "OSPF-Export"
 graceful-restart
 helper-disable
 exit
 area 0.0.0.0
       virtual-link 1.2.3.4 transit-area 1.2.3.4
       hello-interval 9
       dead-interval 40
 exit
 area 0.0.0.20
       stub
 exit
 area 0.0.0.25
```
nssa
exit
exit
area 1.2.3.4
exit

A:ALA-49>config>router>ospf#
In OSPF, an interface can be configured to act as a connection between a router and one of its attached networks. An interface includes state information that was obtained from underlying lower level protocols and from the routing protocol itself. An interface to a network is associated with a single IP address and mask (unless the network is an unnumbered point-to-point network). If the address is merely changed, then the OSPF configuration is preserved.

The passive command enables the passive property to and from the OSPF interface where passive interfaces are advertised as OSPF interfaces but do not run the OSPF protocol. By default, only interface addresses that are configured for OSPF are advertised as OSPF interfaces. The passive parameter allows an interface to be advertised as an OSPF interface without running the OSPF protocol. When enabled, the interface will ignore ingress OSPF protocol packets and not transmit any OSPF protocol packets.

An interface can be part of more than one area, as specified in RFC5185. To do this, add the keyword secondary when creating the interface.

Use the following CLI syntax to configure an OSPF interface:

**CLI Syntax:**

```
ospf ospf-instance
area area-id
  interface ip-int-name
    advertise-subnet
    authentication-key [authentication-key|hash-key]
    [hash|hash2]
    authentication-type [password|message-digest]
    bfd-enable
    dead-interval seconds
    hello-interval seconds
    interface-type {broadcast|point-to-point}
    message-digest-key key-id md5 [key|hash-key][hash|hash2]
    metric metric
    mtu bytes
    passive
    priority number
    retransmit-interval seconds
    no shutdown
    transit-delay seconds
```

The following displays an interface configuration example:

```
A:ALA-49>config>router>ospf# info
----------------------------------------------
asbr
overload
overload-on-boot timeout 60
```
traffic-engineering
export "OSPF-Export"
graceful-restart
    helper-disable
exit
area 0.0.0.0
    virtual-link 1.2.3.4 transit-area 1.2.3.4
    hello-interval 9
    dead-interval 40
exit
interface "system"
exit
area 0.0.0.20
    stub
exit
interface "to-103"
exit
area 0.0.0.25
    nssa
exit
area 1.2.3.4
exit
area 4.3.2.1
    interface "SR1-3"
exit
area 4.3.2.1
    interface "SR1-3" secondary
exit
exit
----------------------------------------------
A:ALA-49>config>router>ospf# area 0.0.0.20
Configuring Authentication

Authentication must be explicitly configured. The following authentication commands can be configured on the interface level or the virtual link level:

- **authentication-key** — Configures the password used by the OSPF interface or virtual-link to send and receive OSPF protocol packets on the interface when simple password authentication is configured.
- **authentication-type** — Enables authentication and specifies the type of authentication to be used on the OSPF interface, either password or message digest.
- **message-digest-key** — Use this command when message-digest keyword is selected in the authentication-type command. The Message Digest 5 (MD5) hashing algorithm is used for authentication. MD5 is used to verify data integrity by creating a 128-bit message digest from the data input. It is unique to that specific data.

An special checksum is included in transmitted packets and are used by the far-end router to verify the packet by using an authentication key (a password). Routers on both ends must use the same MD5 key.

MD5 can be configured on each interface and each virtual link. If MD5 is enabled on an interface, then that interface accepts routing updates only if the MD5 authentication is accepted. Updates that are not authenticated are rejected. A router accepts only OSPF packets sent with the same key-id value defined for the interface.

When the hash parameter is not used, non-encrypted characters can be entered. Once configured using the message-digest-key command, then all keys specified in the command are stored in encrypted format in the configuration file using the hash keyword. When using the hash keyword the password must be entered in encrypted form. Hashing cannot be reversed. Issue the no message-digest-key key-id command and then re-enter the command without the hash parameter to configure an unhashed key.

The following CLI commands are displayed to illustrate the key authentication features. These command parameters can be defined at the same time interfaces and virtual-links are being configured. See Configuring an Interface on page 323 and Configuring a Virtual Link on page 321.

Use the following CLI syntax to configure authentication:

**CLI Syntax:**
```
ospf ospf-instance
area area-id
  interface ip-int-name
    authentication-key [authentication-key|hash-key] [hash]
    authentication-type [password|message-digest]
    message-digest-key key-id md5 key [hash]
virtual-link router-id transit-area area-id
```
Configuring OSPF Components

authentication-key [authentication-key|hash-key]
[has]
authentication-type [password|message-digest]
message-digest-key key-id md5 key [hash]

The following displays authentication configuration examples:

A:ALA-49>config>router>ospf# info
----------------------------------------------
asbr
overload
overload-on-boot timeout 60
traffic-engineering
export "OSPF-Export"
graceful-restart
helper-disable
exit
area 0.0.0.0
   virtual-link 1.2.3.4 transit-area 1.2.3.4
   hello-interval 9
   dead-interval 40
   exit
interface "system"
exit
exit
area 0.0.0.20
   stub
   exit
interface "to-103"
exit
exit
area 0.0.0.25
   nssa
   exit
exit
area 0.0.0.40
   interface "test1"
   authentication-type password
   authentication-key "3WeREdoozyQ" hash
   exit
exit
area 1.2.3.4
exit
----------------------------------------------

A:ALA-49>config>router>ospf# info
----------------------------------------------
asbr
overload
overload-on-boot timeout 60
traffic-engineering
export "OSPF-Export"
graceful-restart
helper-disable
exit
area 0.0.0.0
  virtual-link 10.0.0.1 transit-area 0.0.0.1
    authentication-type message-digest
    message-digest-key 2 md5 "Mi6BQAFi3MI" hash
  exit
  virtual-link 1.2.3.4 transit-area 1.2.3.4
    hello-interval 9
    dead-interval 40
  exit
  interface "system"
  exit
exit
area 0.0.0.1
exit
area 0.0.0.20
  stub
  exit
  interface "to-103"
  exit
exit
area 0.0.0.25
  nssa
  exit
exit
area 0.0.0.40
  interface "test1"
    authentication-type password
    authentication-key "3WErEDozxyQ" hash
  exit
exit
area 1.2.3.4
exit

-----------------------------------------------
A:ALA-49>config>router>ospf#
Assigning a Designated Router

A designated router is elected according to the priority number advertised by the routers. When a router starts up, it checks for a current designated router. If a designated router is present, then the router accepts that designated router, regardless of its own priority designation. When a router fails, then new designated and backup routers are elected according their priority numbers.

The `priority` command is only used if the interface is a broadcast type. The designated router is responsible for flooding network link advertisements on a broadcast network to describe the routers attached to the network. A router uses hello packets to advertise its priority. The router with the highest priority interface becomes the designated router. A router with priority 0 is not eligible to be a designated router or a backup designated router. At least one router on each logical IP network or subnet must be eligible to be the designated router. By default, routers have a priority value of 1.

Use the following CLI syntax to configure the designated router:

**CLI Syntax:**

```
ospf ospf-instance
area area-id
    interface ip-int-name
    priority number
```

The following displays a priority designation example:

```
A:ALA-49>config>router>ospf# info
----------------------------------------------
asbr
overload
overload-on-boot timeout 60
traffic-engineering
export "OSPF-Export"
graceful-restart
    helper-disable
exit
area 0.0.0.0
    virtual-link 10.0.0.1 transit-area 0.0.0.1
    authentication-type message-digest
    message-digest-key 2 md5 "Mi6BQAF13MI" hash
exit
virtual-link 1.2.3.4 transit-area 1.2.3.4
    hello-interval 9
    dead-interval 40
exit
interface "system"
exit
exit
area 0.0.0.1
exit
area 0.0.0.20
    stub
exit
interface "to-103"
```
exit
exit
area 0.0.0.25
    nssa
    exit
    interface "if2"
    priority 100
    exit
exit
area 0.0.0.40
    interface "test1"
    authentication-type password
    authentication-key "3WErEDozyxQ" hash
    exit
exit
area 1.2.3.4
exit

A:ALA-49>config>router>ospf#
### Configuring Route Summaries

Area border routers send summary (type 3) advertisements into a stub area or NSSA to describe the routes to other areas. This command is particularly useful to reduce the size of the routing and Link State Database (LSDB) tables within the stub or NSSA.

By default, summary route advertisements are sent into the stub area or NSSA. The `no` form of the `summaries` command disables sending summary route advertisements and, in stub areas, the default route is advertised by the area border router.

The following CLI commands are displayed to illustrate route summary features. These command parameters can be defined at the same time stub areas and NSSAs are being configured. See Configuring a Stub Area on page 319 and Configuring a Not-So-Stubby Area on page 320.

Use the following CLI syntax to configure a route summary:

**CLI Syntax:**

```
ospf ospf-instance
  area area-id
    stub
      summaries
    nssa
      summaries
```

The following displays a stub route summary configuration example:

```
A:ALA-49>config>router>ospf# info
----------------------------------------------
asbr
overload
overload-on-boot timeout 60
traffic-engineering
export "OSPF-Export"
graceful-restart
  helper-disable
exit
area 0.0.0.0
  virtual-link 10.0.0.1 transit-area 0.0.0.1
    authentication-type message-digest
    message-digest-key 2 md5 "M16BQAF13MI" hash
  exit
  virtual-link 1.2.3.4 transit-area 1.2.3.4
    hello-interval 9
    dead-interval 40
  exit
  interface "system"
  exit
exit
area 0.0.0.1
exit
area 0.0.0.20
  stub
```
exit
interface "to-103"
exit
exit
area 0.0.0.25
nssa
exit
interface "if2"
priority 100
exit
exit
area 0.0.0.40
interface "test1"
authentication-type password
    authentication-key "3WErEDozyQ" hash
exit
exit
area 1.2.3.4
exit

----------------------------------------------
A:ALAE-49>config>router>ospf#
Configuring Route Preferences

A route can be learned by the router from different protocols, in which case, the costs are not comparable. When this occurs the preference value is used to decide which route is installed in the forwarding table if several protocols calculate routes to the same destination. The route with the lowest preference value is selected.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in Table 9. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

### Table 9: Route Preference Defaults by Route Type

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Preference</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct attached</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Static routes</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF internal</td>
<td>10</td>
<td>Yes(^a)</td>
</tr>
<tr>
<td>IS-IS level 1 internal</td>
<td>15</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 internal</td>
<td>18</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF external</td>
<td>150</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 external</td>
<td>160</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 external</td>
<td>165</td>
<td>Yes</td>
</tr>
<tr>
<td>BGP</td>
<td>170</td>
<td>Yes</td>
</tr>
</tbody>
</table>

\(^a\) Preference for OSPF internal routes is configured with the `preference` command.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the `ecmp` in the `config>router` context.

The following CLI commands are displayed to illustrate route preference features. The command parameters can be defined at the same time you are configuring OSPF. See Configuring OSPF Components on page 317.
Use the following CLI syntax to configure a route preference:

**CLI Syntax:**
```
ospf ospf-instance
preference preference
external-preference preference
```

The following displays a route preference configuration example:

```
A:ALA-49>config>router>ospf# info
----------------------------------------------
asbr
overload
overload-on-boot timeout 60
traffic-engineering
preference 9
external-preference 140
export "OSPF-Export"
graceful-restart
helper-disable
exit
area 0.0.0.0
  virtual-link 10.0.0.1 transit-area 0.0.0.1
  authentication-type message-digest
  message-digest-key 2 md5 "Mi6BFqAFi3MI" hash
  exit
  virtual-link 1.2.3.4 transit-area 1.2.3.4
  hello-interval 9
  dead-interval 40
  exit
  interface "system"
  exit
  exit
  area 0.0.0.1
  exit
  area 0.0.20
  stub
  exit
  interface "to-103"
  exit
  exit
  area 0.0.0.25
  nssa
  exit
  interface "if2"
  priority 100
  exit
  exit
  area 0.0.0.40
  interface "test1"
  authentication-type password
  authentication-key "3WErEDozxyQ" hash
  exit
  exit
  area 1.2.3.4
  exit
----------------------------------------------
```
OSPF Configuration Management Tasks

This section discusses the following OSPF configuration management tasks:

- Modifying a Router ID on page 334
- Deleting a Router ID on page 336
- Modifying OSPF Parameters on page 337

Modifying a Router ID

Since the router ID is defined in the `config>router` context, not in the OSPF configuration context, the protocol instance is not aware of the change. Re-examine the plan detailing the router ID. Changing the router ID on a device could cause configuration inconsistencies if associated values are not also modified.

After you have changed a router ID, manually shut down and restart the protocol using the `shutdown` and `no shutdown` commands in order for the changes to be incorporated.

Use the following CLI syntax to change a router ID number:

**CLI Syntax:** `config>router# router-id router-id`

The following displays a NSSA router ID modification example:

```
A:ALA-49>config>router# info
------------------------------------------
IP Configuration
------------------------------------------
interface "system"
  address 10.10.10.104/32
exit
interface "to-103"
  address 10.0.0.103/24
  port 1/1/1
exit
autonomous-system 100
router-id 10.10.10.104
------------------------------------------
A:ALA-49>config>router#

ALA-48>config>router# info
------------------------------------------
IP Configuration
------------------------------------------
interface "system"
  address 10.10.10.103/32
```
exit
interface "to-104"
    address 10.0.0.104/24
    port 1/1/1
exit
autonomous-system 100
router-id 10.10.10.103

------------------------------
ALA-48>config>router#
Deleting a Router ID

You can modify a router ID, but you cannot delete the parameter. When the `no router router-id` command is issued, the router ID reverts to the default value, the system interface address (which is also the loopback address). If a system interface address is not configured, then the last 32 bits of the chassis MAC address is used as the router ID.
Modifying OSPF Parameters

You can change or remove existing OSPF parameters in the CLI or NMS. The changes are applied immediately.

The following example displays an OSPF modification in which an interface is removed and another interface added.

**Example:**
```
config>router# ospf 1
config>router>ospf# area 0.0.0.20
config>router>ospf>area# no interface "to-103"
config>router>ospf>area# interface "to-HQ"
config>router>ospf>area>if$ priority 50
config>router>ospf>area>if# exit
config>router>ospf>area# exit
```

The following example displays the OSPF configuration with the modifications entered in the previous example:

```
A:ALA-49>config>router>ospf# info

asbr
overload
overload-on-boot timeout 60
traffic-engineering
preference 9
external-preference 140
export "OSPF-Export"
graceful-restart
helper-disable
exit
area 0.0.0.0
  virtual-link 10.0.0.1 transit-area 0.0.0.1
    authentication-type message-digest
    message-digest-key 2 md5 "Mi6BQAFi3MI" hash
    exit
  virtual-link 1.2.3.4 transit-area 1.2.3.4
    hello-interval 9
    dead-interval 40
    exit
  interface "system"
exit
area 0.0.0.1
exit
area 0.0.0.20
  stub
  exit
  interface "to-HQ"
    priority 50
  exit
exit
area 0.0.0.25
```
nssa
exit
interface "if2"
    priority 100
exit
exit
area 0.0.0.40
    interface "test1"
        authentication-type password
        authentication-key "3WErEDozxyQ" hash
exit
exit
area 1.2.3.4
exit

----------------------------------------------
A:ALA-49>config>router>ospf#


OSPF Command Reference

Command Hierarchies

- Configuration Commands on page 339
- Show Commands on page 342
- Clear Commands on page 342
- Debug Commands on page 342

Configuration Commands

```
config
  — router
    — [no] ospf ospf-instance
      — [no] advertise-tunnel-links
      — [no] area area-id
        — area-range ip-prefix/mask [advertise | not-advertise]
        — no area-range ip-prefix/mask
        — [no] blackhole-aggregate
        — [no] interface ip-int-name [secondary]
          — [no] advertise-subnet
          — authentication-key [authentication-key | hash-key] [hash | hash2]
          — no authentication-key
          — authentication-type {password | message-digest}
          — no authentication-type
          — bfd-enable
          — no bfd-enable
          — dead-interval seconds
          — no dead-interval
          — export policy-name [.. policy-name]
          — no export
          — export-limit number [log percentage]
          — no export-limit
          — hello-interval seconds
          — no hello-interval
          — interface-type {broadcast | point-to-point}
          — no interface-type
          — [no] loopfree-alternate-exclude
          — message-digest-key key-id md5 [key | hash-key] [hash | hash2]
          — no message-digest-key key-id
          — metric metric
          — no metric
          — mtu bytes
          — no mtu
          — [no] passive
```
— priority number
— no priority
— retransmit-interval seconds
— no retransmit-interval
— [no] shutdown
— transit-delay seconds
— no transit-delay
— [no] loopfree-alternate-exclude
— [no] nssa
— area-range ip-prefix/mask [advertise | not-advertise]
— no area-range ip-prefix/mask
— area-range ip-prefix/prefix-length [advertise | not-advertise]
— no area-range ip-prefix/prefix-length
— originate-default-route [type-7]
— no originate-default-route
— [no] redistribute-external
— [no] summaries
— [no] stub
— default-metric metric
— no default-metric
— [no] summaries
— [no] virtual-link router-id transit-area area-id
— authentication-key [authentication-key | hash-key] [hash | hash2]
— no authentication-key
— authentication-type {password | message-digest}
— no authentication-type
— dead-interval seconds
— no dead-interval
— hello-interval seconds
— no hello-interval
— message-digest-key key-id md5 [key | hash-key] [hash | hash2]
— no message-digest-key key-id
— retransmit-interval seconds
— no retransmit-interval
— [no] shutdown
— transit-delay seconds
— no transit-delay
— [no] asbr [trace-path domain-id]
— [no] compatible-rfc1583
— [no] disable-ldp-sync
— export policy-name [ policy-name...(up to 5 max)]
— no export
— export-limit number [log percentage]
— no export-limit
— external-db-overflow limit seconds
— no external-db-overflow
— external-preference preference
— no external-preference
— [no] graceful-restart
— [no] helper-disable
— [no] ldp-over-rsvp
— [no] loopfree-alternate
— [no] multicast-import
— [no] opaque-isa
— overload [timeout seconds]
— no overload
— [no] overload-include-stub
— overload-on-boot [timeout seconds]
— no overload-on-boot
— preference preference
— no preference
— reference-bandwidth bandwidth-in-kbps
— no reference-bandwidth
— router-id ip-address
— no router-id
— [no] rsvp-shortcut
— [no] shutdown
— timers
  — [no] lsa-arrival lsa-arrival-time
  — [no] lsa-generate max-lsa-wait [lsa-initial-wait [lsa-second-wait]]
  — [no] spf-wait max-spf-wait [spf-initial-wait [spf-second-wait]]
— [no] traffic-engineering
— [no] unicast-import-disable
Show Commands

```
show
  — router
    — ospf [ospf-instance]
      — area [area-id] [detail] [lfa]
      — database [type {router | network | summary | asbr-summary | external | nssa | all}]
        [area area-id] [adv-router router-id] [link-state-id] [detail]
      — interface [area area-id] [detail]
      — interface [ip-int-name | ip-address] [detail]
      — lfa-coverage
      — neighbor [remote ip-address] [detail]
      — neighbor [ip-int-name] [router-id] [detail]
      — opaque-database [link link-id | area area-id | as] [adv-router router-id] [ls-id] [detail]
      — range [area-id]
      — routes [ip-prefix[/prefix-length]] [type] [detail] [alternative] [summary]
      — spf [lfa]
      — statistics
      — status
      — virtual-link [detail]
      — virtual-neighbor [remote ip-address] [detail]
```

Clear Commands

```
clear
  — router
    — ospf [ospf-instance]
      — database [purge]
      — export
      — neighbor [ip-int-name | ip-address]
      — statistics
```

Debug Commands

```
debug
  — router
    — ospf [ospf-instance]
      — area [area-id]
      — no area
      — area-range [ip-address]
      — no area-range
      — csfp [ip-addr]
      — no csfp
      — [no] graceful-restart
      — interface [ip-int-name | ip-address]
      — no interface
      — leak [ip-address]
      — no leak
      — lsdb [type] [ls-id] [adv-rtr-id] [area area-id]
      — no lsdb
```
— [no] misc
— neighbor [ip-int-name | router-id]
— no neighbor
— nssa-range [ip-address]
— no nssa-range
— packet [packet-type] [ip-address]
— no packet
— rtm [ip-addr]
— no rtm
— spf [type] [dest-addr]
— no spf
— virtual-neighbor [ip-address]
— no virtual-neighbor
Configuration Commands

Generic Commands

shutdown

Syntax  [no] shutdown

Context  config>router>ospf
         config>router>ospf>area>interface
         config>router>ospf>area>virtual-link

Description  The shutdown command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the no shutdown command.

The shutdown command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system generated configuration files.

The no form of the command puts an entity into the administratively enabled state.

Default  OSPF Protocol — The Open Shortest Path First (OSPF) protocol is created in the no shutdown state.

OSPF Interface — When an IP interface is configured as an OSPF interface, OSPF on the interface is in the no shutdown state by default.
**OSPF Global Commands**

**ospf**

**Syntax**

```
[no] ospf ospf-instance
```

**Context**

`config>router`

**Description**

This command configures the router ID for the OSPF instance OSPF.

The router ID configured in the base instance of OSPF overrides the router ID configured in the `config>router` context.

The default value for the base instance is inherited from the configuration in the `config>router` context. When that is not configured the following applies:

1. The system uses the system interface address (which is also the loopback address).
2. If a system interface address is not configured, use the last 32 bits of the chassis MAC address.

This is a required command when configuring multiple instances and the instance being configured is not the base instance. When configuring multiple instances of OSPF there is a risk of loops because networks are advertised by multiple domains configured with multiple interconnections to one another. To avoid this from happening all routers in a domain should be configured with the same domain-id. Each domain (OSPF-instance) should be assigned a specific bit value in the 32-bit tag mask.

The default value for non-base instances is 0.0.0.0 and is invalid, in this case the instance of OSPF will not start. When configuring a new router ID, the instance is not automatically restarted with the new router ID. The next time the instance is initialized, the new router ID is used.

Issue the shutdown and no shutdown commands for the instance for the new router ID to be used, or reboot the entire router.

The `no` form of the command to reverts to the default value.

**Default**

`no ospf`

**Parameters**

`ospf-instance` — Specifies a unique integer that identifies a specific instance of a version of the OSPF protocol running in the router instance specified by the router ID.

**Values**

`1 — 31`

**asbr**

**Syntax**

```
[no] asbr [trace-path domain-id]
```

**Context**

`config>router>ospf`

**Description**

This command configures the router as an Autonomous System Boundary Router (ASBR) if the router is to be used to export routes from the Routing Table Manager (RTM) into this instance of OSPF. Once a router is configured as an ASBR, the export policies into this OSPF domain take effect. If no policies are configured no external routes are redistributed into the OSPF domain.
The **no** form of the command removes the ASBR status and withdraws the routes redistributed from the Routing Table Manager into this instance of OSPF from the link state database.

When configuring multiple instances of OSPF there is a risk of loops because networks are advertised by multiple domains configured with multiple interconnections to one another. To avoid this from happening all routers in a domain should be configured with the same domain-id. Each domain (OSPF-instance) should be assigned a specific bit value in the 32-bit tag mask.

When an external route is originated by an ASBR using an internal OSPF route in a given domain, the corresponding bit is set in the AS-external LSA. As the route gets redistributed from one domain to another, more bits are set in the tag mask, each corresponding to the OSPF domain the route visited. Route redistribution looping is prevented by checking the corresponding bit as part of the export policy; if the bit corresponding to the announcing OSPF process is already set, the route is not exported there.

Domain-IDs are incompatible with any other use of normal tags. The domain ID should be configured with a value between 1 and 31 by each router in a given OSPF domain (OSPF Instance).

When an external route is originated by an ASBR using an internal OSPF route in a given domain, the corresponding (1-31) bit is set in the AS-external LSA. As the route gets redistributed from one domain to another, more bits are set in the tag mask, each corresponding to the OSPF domain the route visited. Route redistribution looping is prevented by checking the corresponding bit as part of the export policy; if the bit corresponding to the announcing OSPF process is already set, the route is not exported there.

<table>
<thead>
<tr>
<th>Default</th>
<th>no asbr — The router is not an ASBR.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameters</strong></td>
<td><strong>domain-id</strong> — Specifies the domain ID.</td>
</tr>
<tr>
<td><strong>Values</strong></td>
<td>1 — 31</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>0</td>
</tr>
</tbody>
</table>

**compatible-rfc1583**

**Syntax**  

[no] compatible-rfc1583

**Context**  

config>router>ospf

**Description**  

This command enables OSPF summary and external route calculations in compliance with RFC1583 and earlier RFCs.

RFC1583 and earlier RFCs use a different method to calculate summary and external route costs. To avoid routing loops, all routers in an OSPF domain should perform the same calculation method.
Although it would be favorable to require all routers to run a more current compliancy level, this command allows the router to use obsolete methods of calculation.

The **no** form of the command enables the post-RFC1583 method of summary and external route calculation.

**Default** `compatible-rfc1583` — RFC1583 compliance is enabled.

### disable-ldp-sync

**Syntax**

```
[no] disable-ldp-sync
```

**Context**

`config>router>ospf`

**Description**

This command disables the IGP-LDP synchronization feature on all interfaces participating in the OSPF routing protocol. When this command is executed, IGP immediately advertises the actual value of the link cost for all interfaces which have the IGP-LDP synchronization enabled if the currently advertised cost is different. It will then disable IGP-LDP synchronization for all interfaces. This command does not delete the interface configuration. The **no** form of this command has to be entered to re-enable IGP-LDP synchronization for this routing protocol.

The **no** form of this command restores the default settings and re-enables IGP-LDP synchronization on all interfaces participating in the OSPF or IS-IS routing protocol and for which the ldp-sync-timer is configured.

**Default** `no disable-ldp-sync`

### export

**Syntax**

```
export policy-name [policy-name…]
no export
```

**Context**

`config>router>ospf`

**Description**

This command associates export route policies to determine which routes are exported from the route table to OSPF. Export policies are only in effect if OSPF is configured as an ASBR.

If no export policy is specified, non-OSPF routes are not exported from the routing table manager to OSPF. If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

The **no** form of the command removes all policies from the configuration.

**Default** `no export` — No export route policies specified.

**Parameters**

`policy-name` — The export route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The specified name(s) must already be defined.
export-limit

**Syntax**
```
export-limit number [log percentage]
no export-limit
```

**Context**
```
config>router>ospf
```

**Description**
This command configures the maximum number of routes (prefixes) that can be exported into OSPF from the route table.

The **no** form of the command removes the parameters from the configuration.

**Default**
no export-limit, the export limit for routes or prefixes is disabled.

**Parameters**
- **number** — Specifies the maximum number of routes (prefixes) that can be exported into OSPF from the route table.
  - **Values**
    - 1 — 4294967295

- **log percentage** — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.
  - **Values**
    - 1 — 100

---

external-db-overflow

**Syntax**
```
external-db-overflow limit interval
no external-db-overflow
```

**Context**
```
config>router>ospf
```

**Description**
This command enables limits on the number of non-default AS-external-LSA entries that can be stored in the LSDB and specifies a wait timer before processing these after the limit is exceeded.

The **limit** value specifies the maximum number of non-default AS-external-LSA entries that can be stored in the link-state database (LSDB). Placing a limit on the non-default AS-external-LSAs in the LSDB protects the router from receiving an excessive number of external routes that consume excessive memory or CPU resources. If the number of routes reach or exceed the **limit**, the table is in an overflow state. When in an overflow state, the router will not originate any new AS-external-LSAs. In fact, it withdraws all the self-originated non-default external LSAs.

The **interval** specifies the amount of time to wait after an overflow state before regenerating and processing non-default AS-external-LSAs. The waiting period acts like a dampening period preventing the router from continuously running Shortest Path First (SPF) calculations caused by the excessive number of non-default AS-external LSAs.

The **external-db-overflow** must be set identically on all routers attached to any regular OSPF area. OSPF stub areas and not-so-stubby areas (NSSAs) are excluded.

The **no** form of the command disables limiting the number of non-default AS-external-LSA entries.

**Default**
no external-db-overflow — No limit on non-default AS-external-LSA entries.
Parameters

- **limit** — The maximum number of non-default AS-external-LSA entries that can be stored in the LSDB before going into an overflow state expressed as a decimal integer.
  
  **Values**
  
  0 — 2147483674

- **interval** — The number of seconds after entering an overflow state before attempting to process non-default AS-external-LSAs expressed as a decimal integer.
  
  **Values**
  
  0 — 2147483674

**external-preference**

**Syntax**

```
external-preference preference
no external-preference
```

**Context**

config>router>ospf

**Description**

This command configures the preference for OSPF external routes.

A route can be learned by the router from different protocols, in which case, the costs are not comparable. When this occurs the preference is used to decide which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the Table 10, “Route Preference Defaults by Route Type,” on page 351. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the `ecmp` in the config>router context.

The **no** form of the command reverts to the default value.

**Default**

```
external-preference 150
```

— OSPF external routes have a default preference of 150.
**Parameters**

*preference* — The preference for external routes expressed as a decimal integer. Defaults for different route types are listed in Table 10.

**Table 10: Route Preference Defaults by Route Type**

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Preference</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct attached</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Static routes</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF internal</td>
<td>10</td>
<td>Yes*</td>
</tr>
<tr>
<td>IS-IS level 1 internal</td>
<td>15</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 internal</td>
<td>18</td>
<td>Yes</td>
</tr>
<tr>
<td>RIP</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF external</td>
<td>150</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 external</td>
<td>160</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 external</td>
<td>165</td>
<td>Yes</td>
</tr>
<tr>
<td>BGP</td>
<td>170</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Preference for OSPF internal routes is configured with the *preference* command.

**Values**

1 — 255

---

**graceful-restart**

**Syntax**

[no] graceful-restart

**Context**

config>router>ospf
config>router>ospf3

**Description**

This command enables graceful-restart for OSPF. When the control plane of a GR-capable router fails, the neighboring routers (GR helpers) temporarily preserve adjacency information, so packets continue to be forwarded through the failed GR router using the last known routes. If the control plane of the GR router comes back up within the GR timer, then the routing protocols would re-converge to minimize service interruption.

The *no* form of the command disables graceful restart and removes all graceful restart configurations in the OSPF instance.

**Default**

no graceful-restart
**Helper-disable**

**Syntax**  
```plaintext
[no] helper-disable
```

**Context**  
```
config>router>ospf>graceful-restart  
config>router>ospf3>graceful-restart
```

**Description**  
This command disables the helper support for graceful restart.

When **graceful-restart** is enabled, the router can be a helper (meaning that the router is helping a neighbor to restart) or be a restarting router or both. The router supports only helper mode. This facilitates the graceful restart of neighbors but will not act as a restarting router (meaning that the router will not help the neighbors to restart).

The **no helper-disable** command enables helper support and is the default when graceful-restart is enabled.

**Default**  
```
disabled
```

**Ldp-over-rsvp**

**Syntax**  
```plaintext
[no] ldp-over-rsvp
```

**Context**  
```
config>router>ospf
```

**Description**  
This command allows LDP-over-RSVP processing in this OSPF instance.

**Loopfree-alternate**

**Syntax**  
```plaintext
[no] loopfree-alternate
```

**Context**  
```
config>router>ospf  
config>router>ospf3
```

**Description**  
This command enables Loop-Free Alternate (LFA) computation by SPF under the IS-IS routing protocol level or under the OSPF routing protocol instance level.

When this command is enabled, it instructs the IGP SPF to attempt to pre-compute both a primary next-hop and an LFA next-hop for every learned prefix. When found, the LFA next-hop is populated into the routing table along with the primary next-hop for the prefix.

The **no** form of this command disables the LFA computation by IGP SPF.

**Default**  
```
no loopfree-alternate
```
multicast-import

Syntax  
[no] multicast-import

Context  
config>router>ospf

Description  
This command enables the submission of routes into the multicast Route Table Manager (RTM) by OSPF. The no form of the command disables the submission of routes into the multicast RTM.

Default  
no multicast-import

opaque-lsa

Syntax  
[no] opaque-lsa

Context  
config>router>ospf

Description  
This command enables the router’s support for opaque LSA types. The no form of the command disables the support.

overload

Syntax  
overload [timeout seconds]  
no overload

Context  
config>router>ospf

Description  
This command changes the overload state of the local router so that it appears to be overloaded. When overload is enabled, the router can participate in OSPF routing, but is not used for transit traffic. Traffic destined to directly attached interfaces continues to reach the router.

To put the IGP in an overload state enter a timeout value. The IGP will enter the overload state until the timeout timer expires or a no overload command is executed.

If the overload command is encountered during the execution of an overload-on-boot command then this command takes precedence. This could occur as a result of a saved configuration file where both parameters are saved. When the file is saved by the system the overload-on-boot command is saved after the overload command. However, when overload-on-boot is configured under OSPF with no timeout value configured, the router will remain in overload state indefinitely after a reboot.

Use the no form of this command to return to the default. When the no overload command is executed, the overload state is terminated regardless of the reason the protocol entered overload state.

Default  
no overload

Parameters  
timeout seconds — Specifies the number of seconds to reset overloading.

Values  
1 — 1800

Default  
60
overload-include-stub

Syntax  [no] overload-include-stub
Context config>router>ospf
Description This command is used to determine if the OSPF stub networks should be advertised with a maximum metric value when the system goes into overload state for any reason. When enabled, the system uses the maximum metric value. When this command is enabled and the router is in overload, all stub interfaces, including loopback and system interfaces, will be advertised at the maximum metric.
Default  no overload-include-stub

overload-on-boot

Syntax overload-on-boot [timeout seconds]
no overload
Context config>router>ospf
Description When the router is in an overload state, the router is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

- The timeout timer expires.
- A manual override of the current overload state is entered with the no overload command.

The no overload command does not affect the overload-on-boot function.

The no form of the command removes the overload-on-boot functionality from the configuration.

The default timeout value is 60 seconds, which means after 60 seconds overload status the SR will recover (change back to non-overload status). However, when overload-on-boot is configured under OSPF with no timeout value the router will remain in overload state indefinitely after a reboot.

Parameters timeout seconds — Specifies the number of seconds to reset overloading.

Values  1 — 1800
Default  indefinitely in overload.

preference

Syntax preference preference
no preference
Context config>router>ospf

This command configures the preference for OSPF internal routes.

A route can be learned by the router from different protocols, in which case, the costs are not comparable. When this occurs the preference is used to decide which route will be used.
Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in Table 11. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used.

If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of what route to use is determined by the configuration of the `ecmp` in the `config>router context`.

The `no` form of the command reverts to the default value.

**Default**

| Preference | OSPF internal routes have a preference of 10. |

**Parameters**

| preference | The preference for internal routes expressed as a decimal integer. Defaults for different route types are listed in Table 11. |

**Table 11: Route Preference Defaults by Route Type**

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Preference</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct attached</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Static routes</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF internal</td>
<td>10</td>
<td>Yes*</td>
</tr>
<tr>
<td>IS-IS level 1 internal</td>
<td>15</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 internal</td>
<td>18</td>
<td>Yes</td>
</tr>
<tr>
<td>RIP</td>
<td>100</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF external</td>
<td>150</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 external</td>
<td>160</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 external</td>
<td>165</td>
<td>Yes</td>
</tr>
<tr>
<td>BGP</td>
<td>170</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Preference for OSPF internal routes is configured with the `preference` command.

**Values**

1 — 255

---

**reference-bandwidth**

**Syntax**

```
reference-bandwidth bandwidth-in-kbps
no reference-bandwidth
```

**Context**

`config>router>ospf`

**Description**

This command configures the reference bandwidth in kilobits per second (Kbps) that provides the reference for the default costing of interfaces based on their underlying link speed.
The default interface cost is calculated as follows:

\[ \text{cost} = \frac{\text{reference-bandwidth}}{\text{bandwidth}} \]
The default reference-bandwidth is 100,000,000 Kbps or 100 Gbps, so the default auto-cost metrics for various link speeds are as follows:

- 10 Mbs link default cost of 10000
- 100 Mbs link default cost of 1000
- 1 Gbps link default cost of 100
- 10 Gbps link default cost of 10

The reference-bandwidth command assigns a default cost to the interface based on the interface speed. To override this default cost on a particular interface, use the metric metric command in the config>router>ospf>area>interface ip-int-name context.

The no form of the command reverts the reference-bandwidth to the default value.

**Default**

reference-bandwidth 100000000 — Reference bandwidth of 100 Gbps.

**Parameters**

bandwidth-in-kbps — The reference bandwidth in kilobits per second expressed as a decimal integer.

**Values**

1 — 1000000000

---

**router-id**

**Syntax**

router-id ip-address

no router-id

**Context**

config>router>ospf

**Description**

This command configures the router ID for the OSPF instance. This command configures the router ID for the OSPF instance.

When configuring the router ID in the base instance of OSPF it overrides the router ID configured in the config>router context. The default value for the base instance is inherited from the configuration in the config>router context. If the router ID in the config>router context is not configured, the following applies:

- The system uses the system interface address (which is also the loopback address).
- If a system interface address is not configured, use the last 32 bits of the chassis MAC address.

This is a required command when configuring multiple instances and the instance being configured is not the base instance.

When configuring a new router ID, the instance is not automatically restarted with the new router ID. The next time the instance is initialized, the new router ID is used.

To force the new router ID to be used, issue the shutdown and no shutdown commands for the instance, or reboot the entire router.

The no form of the command reverts to the default value.
OSPF Global Commands

**Default**

The default value for non-base instances is 0.0.0.0 and is invalid, in this case the instance of OSPF will not start and when doing a show command an error condition will be displayed.

**Parameters**

*ip-address* — Specifies a 32-bit, unsigned integer uniquely identifying the router in the Autonomous System.

**rsvp-shortcut**

**Syntax**

```plaintext
[no] rsvp-shortcut
```

**Context**

`config>router>ospf`

**Description**

This command enables the use of an RSVP-TE shortcut for resolving IGP routes by IS-IS or OSPF routing protocols.

This command instructs IS-IS or OSPF to include RSVP LSPs originating on this node and terminating on the router-id of a remote node as direct links with a metric equal to the operational metric provided by MPLS.

When `rsvp-shortcut` is enabled at the IGP instance level, all RSVP LSPs originating on this node are eligible by default as long as the destination address of the LSP, as configured in `configure>router>mpls>lsp>to`, corresponds to a router-id of a remote node. RSVP LSPs with a destination address corresponding to an interface address of a remote node are automatically not considered by IS-IS or OSPF. The user can however exclude a specific RSVP LSP from being used as a shortcut for resolving IGP routes by entering the command `config>router>mpls>lsp>no igp-shortcut`.

Also, the SPF in OSPF or IS-IS will only use RSVP LSPs as IGP shortcuts or as endpoints for LDP-over-RSVP. These applications of RSVP LSPs are mutually exclusive at the IGP instance level. If the user enabled both options at the IGP instance level, then the shortcut application takes precedence when the LSP level configuration has both options enabled.

When an IPv4 packet is received on an ingress network interface, a subscriber IES interface, or a regular IES interface, the lookup of the packet in RTM will result in the resolution of the packet to an RSVP LSP if all the following conditions are satisfied:

- RSVP shortcut is enabled on the IGP routing protocol which has a route for the packet's destination address.
- SPF has pre-determined that the IGP path cost using the RSVP LSP shortcut is the best.

In this case, the packet is sent labeled with the label stack corresponding to the NHLFE of the RSVP LSP.

The failure of an RSVP LSP shortcut or of a local interface triggers a full SPF computation which may result in installing a new route over another RSVP LSP shortcut or a regular IP next-hop.

When ECMP is enabled and multiple equal-cost paths exist for the IGP route, the ingress IOM will spray the packets for this route based on hashing routine currently supported for IPv4 packets. Spraying will be performed across a regular IP next-hop and across an RSVP shortcut next-hop as long as the IP path does not go over the tail-end of the RSVP LSP.

The no form of this command disables the resolution of IGP routes using RSVP shortcuts.

**Default**

`no rsvp-shortcut`
advertise-tunnel-links

**Syntax**  
[no] advertise-tunnel-links

**Context**  
config>router>ospf

**Description**  
This command enables the advertisement of RSVP LSP shortcuts into IGP similar to regular links so that other routers in the network can include them in their SPF computations. An LSP must exist in the reverse direction in order for the advertised link to pass the bi-directional link check and be usable by other routers in the network. However, this is not required for the node which originates the LSP.

The LSP is advertised as an unnumbered point-to-point link and the link LSP/LSA has no Traffic Engineering opaque sub-TLVs per RFC 3906.

The **no** form of this command disables the advertisement of RSVP LSP shortcuts into IGP.

**Default**  
no advertise-tunnel-links

super-backbone

**Syntax**  
[no] super-backbone

**Context**  
config>service>vprn>ospf

**Description**  
This command specifies whether CE-PE functionality is required or not. The OSPF super backbone indicates the type of the LSA generated as a result of routes redistributed into OSPF. When enabled, the redistributed routes are injected as summary, external or NSSA LSAs. When disabled, the redistributed routes are injected as either external or NSSA LSAs only.

Refer to the OS Services Guide for syntax and command usage information.

The **no** form of the command disables the super-backbone functionality.

**Default**  
no super-backbone

timers

**Syntax**  
timers

**Context**  
config>router>ospf

**Description**  
This command enables the context that allows for the configuration of OSPF timers. Timers control the delay between receipt of a link state advertisement (LSA) requiring a Dijkstra (Shortest Path First (SPF)) calculation and the minimum time between successive SPF calculations.

Changing the timers affects CPU utilization and network reconvergence times. Lower values reduce convergence time but increase CPU utilization. Higher values reduce CPU utilization but increase reconvergence time.

**Default**  
none
ls-a-arrival

Syntax

```
ls-a-arrival ls-a-arrival-time
no ls-a-arrival
```

Context

config>router>ospf>timers

Description

This parameter defines the minimum delay that must pass between receipt of the same Link State Advertisements (LSAs) arriving from neighbors.

It is recommended that the neighbors configured (lsa-generate) ls-a-second-wait interval is equal or greater then the ls-a-arrival timer configured here.

Use the no form of this command to return to the default.

Default

no ls-a-arrival

Parameters

```
ls-a-arrival-time — Specifies the timer in milliseconds. Values entered that do not match this requirement will be rejected.
```

Values

```
0 — 600000
```

ls-a-generate

Syntax

```
ls-generate max-lsa-wait [ls-a-initial-wait [ls-a-second-wait]]
no ls-a-generate-interval
```

Context

config>router>ospf>timers

Description

This parameter customizes the throttling of OSPF LSA-generation. Timers that determine when to generate the first, second, and subsequent LSAs can be controlled with this command. Subsequent LSAs are generated at increasing intervals of the ls-a-second-wait timer until a maximum value is reached.

Configuring the ls-a-arrival interval to equal or less than the ls-a-second-wait interval configured in the ls-generate command is recommended.

Use the no form of this command to return to the default.

Default

no ls-a-generate

Parameters

```
max-lsa-wait — Specifies the maximum interval, in milliseconds, between two consecutive occurrences of an LSA being generated.
```

Values

```
10 — 600,000
```

Default

5,000 milliseconds

```
ls-a-initial-wait — Specifies the first waiting period between link-state advertisements (LSA) originate(s), in milliseconds. When the LSA exceeds the ls-a-initial-wait timer value and the topology changes, there is no wait period and the LSA is immediately generated.
```
When an LSA is generated, the initial wait period commences. If, within the specified lsa-initial-wait period and another topology change occurs, then the lsa-initial-wait timer applies.

Values 10 — 600000
Default 5,000 milliseconds

lsa-second-wait — Specifies the hold time in milliseconds between the first and second LSA generation. The next topology change is subject to this second wait period. With each subsequent topology change, the wait time doubles (this is 2x the previous wait time.). This assumes that each failure occurs within the relevant wait period.

Values 10 — 600000
Default 5,000 milliseconds

spf-wait

Syntax spf-wait max-spf-wait [spf-initial-wait [spf-second-wait]]
no spf-wait

Context config>router>ospf>timers

Description This command defines the maximum interval between two consecutive SPF calculations in milliseconds. Timers that determine when to initiate the first, second, and subsequent SPF calculations after a topology change occurs can be controlled with this command. Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the spf-second-wait interval. For example, if the spf-second-wait interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, etc., until it reaches the spf-wait value. The SPF interval will stay at the spf-wait value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to spf-initial-wait.

The timer must be entered in increments of 100 milliseconds. Values entered that do not match this requirement will be rejected.

Use the no form of this command to return to the default.

Default no spf-wait

Parameters max-spf-wait — Specifies the maximum interval in milliseconds between two consecutive SPF calculations.

Values 10 — 120000
Default 1000

spf-initial-wait — Specifies the initial SPF calculation delay in milliseconds after a topology change.

Values 10 — 100000
Default 1000

spf-second-wait — Specifies the hold time in milliseconds between the first and second SPF calculation.

Values 10 — 100000
Default 1000
### traffic-engineering

<table>
<thead>
<tr>
<th>Syntax</th>
<th>[no] traffic-engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>config&gt;router&gt;ospf</td>
</tr>
<tr>
<td>Description</td>
<td>This command enables traffic engineering route calculations constrained by nodes or links. Traffic engineering enables the router to perform route calculations constrained by nodes or links. The traffic engineering capabilities of this router are limited to calculations based on link and nodal constraints. The <code>no</code> form of the command disables traffic engineered route calculations.</td>
</tr>
<tr>
<td>Default</td>
<td><code>no traffic-engineering</code> — Traffic engineered route calculations is disabled.</td>
</tr>
</tbody>
</table>

### unicast-import-disable

<table>
<thead>
<tr>
<th>Syntax</th>
<th>[no] unicast-import-disable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context</td>
<td>config&gt;router&gt;ospf</td>
</tr>
<tr>
<td>Description</td>
<td>This command allows one IGP to import its routes into RPF RTM while another IGP imports routes only into the unicast RTM. Import policies can redistribute routes from an IGP protocol into the RPF RTM (the multicast routing table). By default, the IGP routes will not be imported into RPF RTM as such an import policy must be explicitly configured.</td>
</tr>
<tr>
<td>Default</td>
<td><code>disabled</code></td>
</tr>
</tbody>
</table>
OSPF Area Commands

area

Syntax

[no] area area-id

Context

config>router>ospf

Description

This command creates the context to configure an OSPF area. An area is a collection of network segments within an AS that have been administratively grouped together. The area ID can be specified in dotted decimal notation or as a 32-bit decimal integer.

The no form of the command deletes the specified area from the configuration. Deleting the area also removes the OSPF configuration of all the interfaces, virtual-links, and address-ranges etc., that are currently assigned to this area.

Default

no area — No OSPF areas are defined.

Parameters

area-id — The OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

Values

0.0.0.0 — 255.255.255.255 (dotted decimal), 0 — 4294967295 (decimal integer)

area-range

Syntax

area-range ip-prefix/mask [advertise | not-advertise]

no area-range ip-prefix/mask

Context

config>router>ospf>area
config>router>ospf>area>nssa

Description

This command creates ranges of addresses on an Area Border Router (ABR) for the purpose of route summarization or suppression. When a range is created, the range is configured to be advertised or not advertised into other areas. Multiple range commands may be used to summarize or hide different ranges. In the case of overlapping ranges, the most specific range command applies.

ABRs send summary link advertisements to describe routes to other areas. To minimize the number of advertisements that are flooded, you can summarize a range of IP addresses and send reachability information about these addresses in an LSA.

The no form of the command deletes the range (non)advertisement.

Default

no area-range — No range of addresses are defined.

Special Cases

NSSA Context — In the NSSA context, the option specifies that the range applies to external routes (via type-7 LSAs) learned within the NSSA when the routes are advertised to other areas as type-5 LSAs.

Area Context — If this command is not entered under the NSSA context, the range applies to summary LSAs even if the area is an NSSA.
Parameters

*ip-prefix* — The IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

**Values**
ip-prefix/mask: ip-prefix a.b.c.d (host bits must be 0)

*mask* — The subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

**Values**
0 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)

*advertise* | *not-advertise* — Specifies whether or not to advertise the summarized range of addresses into other areas. The *advertise* keyword indicates the range will be advertised, and the keyword *not-advertise* indicates the range will not be advertised. The default is *advertise*.

blackhole-aggregate

**Syntax**

[no] blackhole-aggregate

**Context**
config>router>ospf>area

**Description**
This command installs a low priority blackhole route for the entire aggregate. Existing routes that make up the aggregate will have a higher priority and only the components of the range for which no route exists are blackholed.

It is possible that when performing area aggregation, addresses may be included in the range for which no actual route exists. This can cause routing loops. To avoid this problem configure the blackhole aggregate option.

The *no* form of this command removes this option.

**Default**
blackhole-aggregate

default-metric

**Syntax**
default-metric *metric*

[no] default-metric

**Context**
config>router>ospf>area>stub

**Description**
This command configures the metric used by the area border router (ABR) for the default route into a stub area.

The default metric should only be configured on an ABR of a stub area.

An ABR generates a default route if the area is a *stub* area.

The *no* form of the command reverts to the default value.

**Default**
default-metric 1
**Parameters**  
*metric* — The metric expressed as a decimal integer for the default route cost to be advertised into the stub area.

**Values**  
1 — 16777215

---

**loopfree-alternate-exclude**

**Syntax**  
[no] loopfree-alternate

**Context**  
config>router>ospf>area  
config>router>ospf>area>interface

**Description**  
This command instructs IGP to not include a specific interface or all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

When an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When it is excluded from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

The **no** form of this command re-instates the default value for this command.

**Default**  
no loopfree-alternate-exclude.

---

**nssa**

**Syntax**  
[no] nssa

**Context**  
config>router>ospf>area

**Description**  
This command creates the context to configure an OSPF Not So Stubby Area (NSSA) and adds/removes the NSSA designation from the area.

NSSAs are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is that an NSSA has the capability to flood external routes that it learns throughout its area and via an ABR to the entire OSPF domain.

Existing virtual links of a non-stub or NSSA area will be removed when the designation is changed to NSSA or stub.

An area can be designated as stub or NSSA but never both at the same time.

By default, an area is not configured as an NSSA area.

The **no** form of the command removes the NSSA designation and configuration context from the area.

**Default**  
**no nssa** — The OSPF area is not an NSSA.
**originiate-default-route**

- **Syntax**
  - originate-default-route [type-7]
  - no originate-default-route

- **Context**
  - config>router>ospf>area>nssa

- **Description**
  This command enables the generation of a default route and its LSA type (3 or 7) into a Not So Stubby Area (NSSA) by an NSSA Area Border Router (ABR) or Autonomous System Border Router (ASBR).

  When configuring an NSSA with no summaries, the ABR will inject a type 3 LSA default route into the NSSA area. Some older implementations expect a type 7 LSA default route.

  The no form of the command disables origination of a default route.

- **Default**
  - no originate-default-route — A default route is not originated.

- **Parameters**
  - type-7 — Specifies a type 7 LSA should be used for the default route.

    Configure this parameter to inject a type-7 LSA default route instead of the type 3 LSA into the NSSA configured with no summaries.

    To revert to a type 3 LSA, enter originate-default-route without the type-7 parameter.

- **Default**
  - Type 3 LSA for the default route.

---

**redistribute-external**

- **Syntax**
  - [no] redistribute-external

- **Context**
  - config>router>ospf>area>nssa

- **Description**
  This command enables the redistribution of external routes into the Not So Stubby Area (NSSA) or an NSSA area border router (ABR) that is exporting the routes into non-NSSA areas.

  NSSA or Not So Stubby Areas are similar to stub areas in that no external routes are imported into the area from other OSPF areas. The major difference between a stub area and an NSSA is that the NSSA has the capability to flood external routes that it learns (providing it is an ASBR) throughout its area and via an Area Border Router to the entire OSPF domain.

  The no form of the command disables the default behavior to automatically redistribute external routes into the NSSA area from the NSSA ABR.

- **Default**
  - redistribute-external — External routes are redistributed into the NSSA.
stub

Syntax  [no] stub
Context  config>router>ospf>area
Description  This command enables access to the context to configure an OSPF stub area and adds/removes the stub designation from the area.

External routing information is not flooded into stub areas. All routers in the stub area must be configured with the stub command. An OSPF area cannot be both an NSSA and a stub area.

Existing virtual links of a non STUB or NSSA area will be removed when its designation is changed to NSSA or STUB.

By default, an area is not a stub area.

The no form of the command removes the stub designation and configuration context from the area.

Default  no stub — The area is not configured as a stub area.

summaries

Syntax  [no] summaries
Context  config>router>ospf>area>stub
        config>router>ospf>area>nssa
Description  This command enables sending summary (type 3) advertisements into a stub area or Not So Stubby Area (NSSA) on an Area Border Router (ABR).

This parameter is particularly useful to reduce the size of the routing and Link State Database (LSDB) tables within the stub or NSSA area. (Default: summary)

By default, summary route advertisements are sent into the stub area or NSSA.

The no form of the command disables sending summary route advertisements and, for stub areas, only the default route is advertised by the ABR.

Default  summaries — Summary routes are advertised by the ABR into the stub area or NSSA.
Interface/Virtual Link Commands

advertise-subnet

Syntax  
[no] advertise-subnet

Context  
config>router>ospf>area>interface ip-int-name

Description  
This command enables advertising point-to-point interfaces as subnet routes (network number and mask). When disabled, point-to-point interfaces are advertised as host routes.

The no form of the command disables advertising point-to-point interfaces as subnet routes meaning they are advertised as host routes.

Default   
advertise-subnet — Advertises point-to-point interfaces as subnet routes.

authentication-key

Syntax  
authentication-key [authentication-key | hash-key] [hash | hash2]

no authentication-key

Context  
config>router>ospf>area>interface ip-int-name
config>router>ospf>area>virtual-link >if>

Description  
This command configures the password used by the OSPF interface or virtual-link to send and receive OSPF protocol packets on the interface when simple password authentication is configured.

All neighboring routers must use the same type of authentication and password for proper protocol communication. If the authentication-type is configured as password, then this key must be configured.

By default, no authentication key is configured.

The no form of the command removes the authentication key.

Default   
no authentication-key — No authentication key is defined.

Parameters  
authentication-key — The authentication key. The key can be any combination of ASCII characters up to 8 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 22 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.
hash2 — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.

**authentication-type**

**Syntax**
```
authentication-type {password | message-digest}
no authentication-type
```

**Context**
```
config>router>ospf>area>interface ip-int-name
config>router>ospf>area>virtual-link router-id
```

**Description**
This command enables authentication and specifies the type of authentication to be used on the OSPF interface.

Both simple `password` and `message-digest` authentication are supported.

By default, authentication is not enabled on an interface.

The `no` form of the command disables authentication on the interface.

**Default**
`no authentication` — No authentication is enabled on an interface.

**Parameters**
`password` — This keyword enables simple password (plain text) authentication. If authentication is enabled and no authentication type is specified in the command, simple `password` authentication is enabled.

`message-digest` — This keyword enables message digest MD5 authentication in accordance with RFC1321. If this option is configured, then at least one message-digest-key must be configured.

**bfd-enable**

**Syntax**
```
[no] bfd-enable [remain-down-on-failure]
```

**Context**
```
config>router>ospf>area>interface
config>router>ospf3>area>interface
```

**Description**
This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The `no` form of this command removes BFD from the associated IGP protocol adjacency.

**Default**
`no bfd-enable`

**Parameters**
`remain-down-on-failure` — Forces adjacency down on BFD failure.
dead-interval

Syntax  dead-interval seconds
        no dead-interval

Context  config>router>ospf>area>interface
        config>router>ospf>area>virtual-link

Description  This command configures the time, in seconds, that OSPF waits before declaring a neighbor router down. If no hello packets are received from a neighbor for the duration of the dead interval, the router is assumed to be down. The minimum interval must be two times the hello interval.

        The no form of the command reverts to the default value.

Default  40 seconds

Special Cases  OSPF Interface — If the dead-interval configured applies to an interface, then all nodes on the subnet must have the same dead interval.

        Virtual Link — If the dead-interval configured applies to a virtual link, then the interval on both termination points of the virtual link must have the same dead interval.

Parameters  seconds — The dead interval expressed in seconds.

Values  1 — 65535

export

Syntax  [no] export policy-name [policy-name...up to 5 max]

Context  config>router>ospf

Description  This command configures export routing policies that determine the routes exported from the routing table to OSPF.

        If no export policy is defined, non OSPF routes are not exported from the routing table manager to IS-IS.

        If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered overrides the previous command. A maximum of five policy names can be specified.

        If an aggregate command is also configured in the config>router context, then the aggregation is applied before the export policy is applied.

        Routing policies are created in the config>router>policy-options context.

        The no form of the command removes the specified policy-name or all policies from the configuration if no policy-name is specified.

Default  no export — No export policy name is specified.

Parameters  policy-name — The export policy name. Up to five policy-name arguments can be specified.
export-limit

Syntax

export-limit number [log percentage]
no export-limit

Context
config>router>ospf

Description
This command configures the maximum number of routes (prefixes) that can be exported into OSPF from the route table.

The no form of the command removes the parameters from the configuration.

Default
no export-limit, the export limit for routes or prefixes is disabled.

Parameters
number — Specifies the maximum number of routes (prefixes) that can be exported into OSPF from the route table.

Values
1 — 4294967295

log percentage — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.

Values
1 — 100

hello-interval

Syntax

hello-interval seconds
no hello-interval

Context
config>router>ospf>area>interface
config>router>ospf>area>virtual-link

Description
This command configures the interval between OSPF hellos issued on the interface or virtual link.

The hello interval, in combination with the dead-interval, is used to establish and maintain the adjacency. Use this parameter to edit the frequency that hello packets are sent.

Reducing the interval, in combination with an appropriate reduction in the associated dead-interval, allows for faster detection of link and/or router failures at the cost of higher processing costs.

The no form of this command reverts to the default value.

Default
hello-interval 10 — A 10-second hello interval.

Special Cases
OSPF Interface — If the hello-interval configured applies to an interface, then all nodes on the subnet must have the same hello interval.

Virtual Link — If the hello-interval configured applies to a virtual link, then the interval on both termination points of the virtual link must have the same hello interval.

Parameters
seconds — The hello interval in seconds expressed as a decimal integer.

Values
1 — 65535
interface

**Syntax**  
[no] interface ip-int-name [secondary]

**Context**  
config>router>ospf>area

**Description**  
This command creates a context to configure an OSPF interface.

By default, interfaces are not activated in any interior gateway protocol, such as OSPF, unless explicitly configured.

The no form of the command deletes the OSPF interface configuration for this interface. The shutdown command in the config>router>ospf>interface context can be used to disable an interface without removing the configuration for the interface.

**Default**  
no interface — No OSPF interfaces are defined.

**Parameters**

- **ip-int-name** — The IP interface name. Interface names must be unique within the group of defined IP interfaces for config router interface and config service ies interface commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

- If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

- If the IP interface exists in a different area it will be moved to this area.

- secondary — Allows multiple secondary adjacencies to be established over a single IP interface.

interface-type

**Syntax**

interface-type {broadcast | point-to-point}
no interface-type

**Context**  
config>router>ospf>area>interface

**Description**  
This command configures the interface type to be either broadcast or point-to-point.

Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the broadcast adjacency maintenance overhead of the Ethernet link provided the link is used as a point-to-point.

If the interface type is not known at the time the interface is added to OSPF and subsequently the IP interface is bound (or moved) to a different interface type, this command must be entered manually.

The no form of the command reverts to the default value.

**Default**  
point-to-point if the physical interface is SONET.

broadcast if the physical interface is Ethernet or unknown.

**Special Cases**

Virtual-Link — A virtual link is always regarded as a point-to-point interface and not configurable.
Parameters

**broadcast** — Configures the interface to maintain this link as a broadcast network. To significantly improve adjacency forming and network convergence, a network should be configured as point-to-point if only two routers are connected, even if the network is a broadcast media such as Ethernet.

**point-to-point** — Configures the interface to maintain this link as a point-to-point link.

**message-digest-key**

**Syntax**

```
message-digest-key keyid md5 [key | hash-key] [hash]
no message-digest-key keyid
```

**Context**

```
config>router>ospf>area>interface
config>router>ospf>area>virtual-link
```

**Description**

This command configures a message digest key when MD5 authentication is enabled on the interface. Multiple message digest keys can be configured.

The **no** form of the command removes the message digest key identified by the **key-id**.

**Default**

No message digest keys are defined.

**Parameters**

**keyid** — The **keyid** is expressed as a decimal integer.

- **Values**
  - 1 — 255

**md5**

**key** — The MD5 key. The **key** can be any alphanumeric string up to 16 characters in length.

**md5**

**hash-key** — The MD5 hash key. The key can be any combination of ASCII characters up to 32 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

**hash** — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

**metric**

**Syntax**

```
metric metric
no metric
```

**Context**

```
config>router>ospf>area>interface
```

**Description**

This command configures an explicit route cost metric for the OSPF interface that overrides the metrics calculated based on the speed of the underlying link.

The **no** form of the command deletes the manually configured interface metric, so the interface uses the computed metric based on the **reference-bandwidth** command setting and the speed of the underlying link.

**Default**

**no metric** — The metric is based on **reference-bandwidth** setting and the link speed.
Interface/Virtual Link Commands

**Parameters**

*metric* — The metric to be applied to the interface expressed as a decimal integer.

**Values**

1 — 65535

**mtu**

**Syntax**

mtu bytes

no mtu

**Context**

config>router>ospf>area>interface

**Description**

This command configures the OSPF packet size used on this interface. If this parameter is not configured OSPF derives the MTU value from the MTU configured (default or explicitly) in the following contexts:

config>port>ethernet
config>port>sonet-sdh>path

If this parameter is configured, the smaller value between the value configured here and the MTU configured (default or explicitly) in an above-mentioned context is used.

To determine the actual packet size add 14 bytes for an Ethernet packet and 18 bytes for a tagged Ethernet packet to the size of the OSPF (IP) packet MTU configured in this command.

Use the **no** form of this command to revert to default.

**Default**

no mtu — Uses the value derived from the MTU configured in the config>port context.

**Parameters**

*bytes* — The MTU to be used by OSPF for this logical interface in bytes.

**Values**

512 — 9198 (9212 — 14) (Depends on the physical media)

**passive**

**Syntax**

[no] passive

**Context**

config>router>ospf>area>interface

**Description**

This command adds the passive property to the OSPF interface where passive interfaces are advertised as OSPF interfaces but do not run the OSPF protocol.

By default, only interface addresses that are configured for OSPF will be advertised as OSPF interfaces. The **passive** parameter allows an interface to be advertised as an OSPF interface without running the OSPF protocol.

While in passive mode, the interface will ignore ingress OSPF protocol packets and not transmit any OSPF protocol packets.

The **no** form of the command removes the passive property from the OSPF interface.

**Default**

Service interfaces defined in config>router>service-prefix are passive.

All other interfaces are not passive.
priority

**Syntax**  
`priority number`  
`no priority`

**Context**  
`config>router>ospf>area>interface`

**Description**  
This command configures the priority of the OSPF interface that is used in an election of the designated router on the subnet.

This parameter is only used if the interface is of type broadcast. The router with the highest priority interface becomes the designated router. A router with priority 0 is not eligible to be Designated Router or Backup Designated Router.

The `no` form of the command reverts the interface priority to the default value.

**Default**  
`priority 1`

**Parameters**  
`number` — The interface priority expressed as a decimal integer. A value of 0 indicates the router is not eligible to be the Designated Router or Backup Designated Router on the interface subnet.

**Values**  
0 — 255

retransmit-interval

**Syntax**  
`retransmit-interval seconds`  
`no retransmit-interval`

**Context**  
`config>router>ospf>area>interface`

`config>router>ospf>area>virtual-link`

**Description**  
This command specifies the length of time, in seconds, that OSPF will wait before retransmitting an unacknowledged link state advertisement (LSA) to an OSPF neighbor.

The value should be longer than the expected round trip delay between any two routers on the attached network. Once the retransmit-interval expires and no acknowledgement has been received, the LSA will be retransmitted.

The `no` form of this command reverts to the default interval.

**Default**  
`retransmit-interval 5`

**Parameters**  
`seconds` — The retransmit interval in seconds expressed as a decimal integer.

**Values**  
1 — 1800
transit-delay

**Syntax**

```
transit-delay seconds
no transit-delay
```

**Context**

```
config>router>ospf>area>interface
config>router>ospf>area>virtual-link
```

**Description**

This command configures the estimated time, in seconds, that it takes to transmit a link state advertisement (LSA) on the interface or virtual link.

The `no` form of this command reverts to the default delay time.

**Default**

```
transit-delay 1
```

**Parameters**

- `seconds` — The transit delay in seconds expressed as a decimal integer.

  **Values**

  1 — 1800

virtual-link

**Syntax**

```
[no] virtual-link router-id transit-area area-id
```

**Context**

```
config>router>ospf>area
```

**Description**

This command configures a virtual link to connect area border routers to the backbone via a virtual link.

The backbone area (area 0.0.0.0) must be contiguous and all other areas must be connected to the backbone area. If it is not practical to connect an area to the backbone (see area 0.0.0.2 in the picture below) then the area border routers (routers 1 and 2 in the picture below) must be connected via a virtual link. The two area border routers will form a point-to-point like adjacency across the transit area. (area 0.0.0.1 in the picture below). A virtual link can only be configured while in the area 0.0.0.0 context.

The `router-id` specified in this command must be associated with the virtual neighbor. The transit area cannot be a stub area or a Not So Stubby Area (NSSA).

The `no` form of the command deletes the virtual link. *(Default: none specified)*

**Default**

No virtual link is defined.

**Parameters**

- `router-id` — The router ID of the virtual neighbor in IP address dotted decimal notation.

- `transit-area area-id` — The area-id specified identifies the transit area that links the backbone area with the area that has no physical connection with the backbone.

  The OSPF backbone area, area 0.0.0.0, must be contiguous and all other areas must be connected to the backbone area. The backbone distributes routing information between areas. If it is not practical to connect an area to the backbone (see Area 0.0.0.5 in Figure 13) then the area border routers (such as routers Y and Z) must be connected via a virtual link. The two area border routers form a point-to-point-like adjacency across the transit area (see Area 0.0.0.4).
Figure 13: OSPF Areas
Show Commands

ospf

Syntax  ospf [ospf-instance]
Context  show>router
Description  This command enables the context to display OSPF information.
Parameters  ospf-instance — Clears the configured specified VR-ID.
  Values  1 — 4294967295

area

Syntax  area [area-id] [detail] [lfa]
Context  show>router>ospf
Description  This command displays configuration information about all areas or the specified area. When detail is specified operational and statistical information will be displayed.
Parameters  area-id — The OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.
  detail — Displays detailed information about the specified area.
  lfa — Displays Loop-Free Alternate (LFA) next-hop information.
Output  OSPF Area Output — The following table describes the standard and detailed command output fields for an OSPF area.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Id</td>
<td>A 32 bit integer uniquely identifying an area.</td>
</tr>
<tr>
<td>Type</td>
<td>NSSA — This area is configured as an NSSA area.</td>
</tr>
<tr>
<td></td>
<td>Standard — This area is configured as a standard area (not NSSA or Stub).</td>
</tr>
<tr>
<td></td>
<td>Stub — This area is configured as a stub area.</td>
</tr>
<tr>
<td>SPF Runs</td>
<td>The number of times that the intra-area route table has been calculated using this area’s link state database.</td>
</tr>
<tr>
<td>LSA Count</td>
<td>The total number of link-state advertisements in this area’s link state database, excluding AS External LSA’s.</td>
</tr>
</tbody>
</table>
### Sample Output

```mermaid
A:SetupCLI# show router ospf area detail
```

### Show Commands

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSA Cksum Sum</td>
<td>The 32-bit unsigned sum of the link-state database advertisements LS checksums contained in this area’s link state database. This checksum excludes AS External LSAs (type-5).</td>
</tr>
<tr>
<td>No. of OSPF Areas</td>
<td>The number of areas configured on the router.</td>
</tr>
<tr>
<td>Virtual Links</td>
<td>The number of virtual links configured through this transit area.</td>
</tr>
<tr>
<td>Active IFs</td>
<td>The active number of interfaces configured in this area.</td>
</tr>
<tr>
<td>Area Bdr Rtrs</td>
<td>The total number of ABRs reachable within this area.</td>
</tr>
<tr>
<td>AS Bdr Rtrs</td>
<td>The total number of ASBRs reachable within this area.</td>
</tr>
<tr>
<td>Last SPF Run</td>
<td>The time when the last intra-area SPF was run on this area.</td>
</tr>
<tr>
<td>Router LSAs</td>
<td>The total number of router LSAs in this area.</td>
</tr>
<tr>
<td>Network LSAs</td>
<td>The total number of network LSAs in this area.</td>
</tr>
<tr>
<td>Summary LSAs</td>
<td>The summary of LSAs in this area.</td>
</tr>
<tr>
<td>Asbr-summ LSAs</td>
<td>The summary of ASBR LSAs in this area.</td>
</tr>
<tr>
<td>Nssa-ext LSAs</td>
<td>The total number of NSSA-EXT LSAs in this area.</td>
</tr>
<tr>
<td>Area opaque LSAs</td>
<td>The total number of opaque LSAs in this area.</td>
</tr>
<tr>
<td>Total Nbrs</td>
<td>The total number of neighbors in this area.</td>
</tr>
<tr>
<td>Total IFs</td>
<td>The total number of interfaces configured in this area.</td>
</tr>
<tr>
<td>Total LSAs</td>
<td>The sum of LSAs in this area excluding autonomous system external LSAs.</td>
</tr>
<tr>
<td>Blackhole Range</td>
<td>False — No blackhole route is installed for aggregates configured in this area.</td>
</tr>
<tr>
<td></td>
<td>True — A lowest priority blackhole route is installed for aggregates configured in this area.</td>
</tr>
</tbody>
</table>

#### Blackhole Range

- **False** — No blackhole route is installed for aggregates configured in this area.
- **True** — A lowest priority blackhole route is installed for aggregates configured in this area.
<table>
<thead>
<tr>
<th>Area Id</th>
<th>Area Id</th>
<th>Type</th>
<th>Virtual Links</th>
<th>Active IFs</th>
<th>Area Bdr Rtrs</th>
<th>SPF Runs</th>
<th>Router LSAs</th>
<th>Summary LSAs</th>
<th>Nssa ext LSAs</th>
<th>Total LSAs</th>
<th>Blackhole Range</th>
<th>LSA Cksum Sum</th>
<th>Unknown LSAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>1.1.1.1</td>
<td>Stub</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>True</td>
<td>0x6af</td>
<td>0</td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>2.2.2.2</td>
<td>Standard</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>False</td>
<td>0x493</td>
<td>0</td>
</tr>
</tbody>
</table>

**A:SetupCLI#**

**A:SR# show router ospf area detail**

**OSPF Areas (Detailed)**

**Area Id: 0.0.0.0**

<table>
<thead>
<tr>
<th>Area Id</th>
<th>Area Id</th>
<th>Type</th>
<th>Virtual Links</th>
<th>Active IFs</th>
<th>Area Bdr Rtrs</th>
<th>SPF Runs</th>
<th>Router LSAs</th>
<th>Summary LSAs</th>
<th>Nssa ext LSAs</th>
<th>Total LSAs</th>
<th>Blackhole Range</th>
<th>LSA Cksum Sum</th>
<th>Unknown LSAs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>Standard</td>
<td>0</td>
<td>3</td>
<td>0</td>
<td>7</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>9</td>
<td>True</td>
<td>0x28b62</td>
<td>0</td>
</tr>
</tbody>
</table>

*A:Bombadil# show router ospf area 0.0.0.0 detail*
Show Commands

OSPF Area (Detailed) : 0.0.0.0

Configuration

Area Id          : 0.0.0.0              Type             : Standard

Statistics

Virtual Links    : 0                    Total Nbrs       : 2
Active IFs       : 3                    Total IFs        : 3
Area Bdr Rtrs    : 0                    AS Bdr Rtrs      : 0
SPF Runs         : 7                    Last SPF Run     : 10/26/2006 10:09:18
Router LSAs      : 3                    Network LSAs     : 3
Summary LSAs     : 0                    Asbr-summ LSAs   : 0
Nssa ext LSAs    : 0                    Area opaque LSAs : 3
Total LSAs       : 9                    LSA Cksum Sum    : 0x28b62
Blackhole Range  : True                 Unknown LSAs     : 0

*A:Dut-B# show router ospf area 0.0.0.0 lfa

Path Table

Node               Interface                     Nexthop
LFA Interface                 LFA Nexthop
-----------------------------------------------------------------------
10.20.1.1           to_Dut-A1                     10.20.1.1
                      to_Dut-C1                     10.20.1.3
10.20.1.3           to_Dut-C1                     10.20.1.3
                      to_Dut-A1                     10.20.1.1
10.20.1.4           to_Dut-D1                     10.20.1.4
10.20.1.6           to_Dut-D1                     10.20.1.4
                      to_Dut-C1                     10.20.1.3

*A:Dut-B#

*A:Dut-B# show router ospf area 0.0.0.0 lfa detail

Path Table

OSPF Area : 0.0.0.0

Node : 10.20.1.1          Metric             : 10
Interface : to_Dut-A1          Nexthop : 10.20.1.1
LFA Interface : to_Dut-C1          LFA Metric : 20
LFA type : linkProtection          LFA Nexthop : 10.20.1.3

Node : 10.20.1.3          Metric             : 10
Interface : to_Dut-C1          Nexthop : 10.20.1.3
LFA Interface : to_Dut-A1          LFA Metric : 20
LFA type : linkProtection          LFA Nexthop : 10.20.1.1

Node : 10.20.1.4          Metric             : 10
database

Syntax  
```
database [type {router | network | summary | asbr-summary | external | nssa | all}] [area area-id] [adv-router router-id] [link-state-id] [detail]
```

Context  
```
show>router>ospf
```

Description  
This command displays information about the OSPF link state database (LSDB).
When no command line options are specified, the command displays brief output for all database entries

Parameters  
```
ospf-instance — The OSPF instance.
```

Values  
```
1 — 4294967295
```

```
type keyword — Specifies to filter the OSPF LSDB information based on the type specified by keyword.
type router — Display only router (Type 1) LSAs in the LSDB.
type network — Display only network (Type 2) LSAs in the LSDB.
type summary — Display only summary (Type 3) LSAs in the LSDB.
type asbr-summary — Display only ASBR summary (Type 4) LSAs in the LSDB.
type external — Display only AS external (Type 5) LSAs in the LSDB. External LSAs are maintained
globally and not per area. If the display of external links is requested, the area parameter, if present, is
ignored.
type nssa — Displays only NSSA area-specific AS external (Type 7) LSAs in the LSDB.
type all — Display all LSAs in the LSDB. The all keyword is intended to be used with either the area area-
id or the adv-router router-id [link-state-id] parameters.
area area-id — Display LSDB information associated with the specified OSPF area-id.
adv-router router-id [link-state-id] — Display LSDB information associated with the specified advertising
router. To further narrow the number of items displayed, the link-state-id can optionally be specified.
detail — Displays detailed information on the LSDB entries.
### OSPF Database Output

The following table describes the standard and detailed command output fields for an OSPF database.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Area Id</strong></td>
<td>The OSPF area identifier.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td><strong>Router</strong> — LSA type of router (OSPF)</td>
</tr>
<tr>
<td><strong>LSA Type</strong></td>
<td><strong>Network</strong> — LSA type of network (OSPF)</td>
</tr>
<tr>
<td></td>
<td><strong>Summary</strong> — LSA type of summary (OSPF)</td>
</tr>
<tr>
<td></td>
<td><strong>ASBR Summary</strong> — LSA type of ASBR summary (OSPF)</td>
</tr>
<tr>
<td></td>
<td><strong>Nssa-ext</strong> — LSA area-specific, NSSA external (OSPF)</td>
</tr>
<tr>
<td></td>
<td><strong>Area opaque</strong> — LSA type of area opaque (OSPF)</td>
</tr>
<tr>
<td><strong>Link State Id</strong></td>
<td>The link state Id is an LSA type specific field containing either a number</td>
</tr>
<tr>
<td></td>
<td>to distinguish several LSAs from the same router, an interface ID, or a</td>
</tr>
<tr>
<td></td>
<td>router-id; it identifies the piece of the routing domain being</td>
</tr>
<tr>
<td></td>
<td>described by the advertisement.</td>
</tr>
<tr>
<td><strong>Adv Rtr Id</strong></td>
<td>The router identifier of the router advertising the LSA.</td>
</tr>
<tr>
<td><strong>Adv Router Id</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td>The age of the link state advertisement in seconds.</td>
</tr>
<tr>
<td><strong>Sequence</strong></td>
<td>The signed 32-bit integer sequence number.</td>
</tr>
<tr>
<td><strong>Sequence No</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Checksum</strong></td>
<td>The 32-bit unsigned sum of the link-state advertisements' LS checksums.</td>
</tr>
<tr>
<td><strong>Checksum</strong></td>
<td></td>
</tr>
<tr>
<td><strong>No. of LSAs</strong></td>
<td>The number of LSAs displayed.</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td><strong>EA</strong> — External Attribute LSA Support</td>
</tr>
<tr>
<td></td>
<td><strong>DC</strong> — Demand Circuit Support</td>
</tr>
<tr>
<td></td>
<td><strong>R</strong> — If clear, a node can participates in OSPF topology distribution</td>
</tr>
<tr>
<td></td>
<td>without being used to forward transit traffic.</td>
</tr>
<tr>
<td></td>
<td><strong>N</strong> — Type 7 LSA Support</td>
</tr>
<tr>
<td></td>
<td><strong>MC</strong> — Multicast Support</td>
</tr>
<tr>
<td></td>
<td><strong>E</strong> — External Routes Support</td>
</tr>
<tr>
<td><strong>Prefix Options</strong></td>
<td><strong>P</strong> — Propagate NSSA LSA.</td>
</tr>
<tr>
<td></td>
<td><strong>MC</strong> — Multicast support</td>
</tr>
</tbody>
</table>
### Sample Output

A:ALA-A# `show router ospf 1 database`

```
OSPF Link State Database (Type : All)

<table>
<thead>
<tr>
<th>Area Id</th>
<th>Type</th>
<th>Link State Id</th>
<th>Adv Rtr Id</th>
<th>Age</th>
<th>Sequence</th>
<th>Cksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>180.0.0.2</td>
<td>180.0.0.2</td>
<td>1800</td>
<td>0x800000b6</td>
<td>0xf54</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>180.0.0.5</td>
<td>180.0.0.5</td>
<td>1902</td>
<td>0x80000099</td>
<td>0xcb7c</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>180.0.0.8</td>
<td>180.0.0.8</td>
<td>1815</td>
<td>0x80000099</td>
<td>0x529b</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>180.0.0.9</td>
<td>180.0.0.9</td>
<td>1156</td>
<td>0x80000085</td>
<td>0x529b</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>180.0.0.10</td>
<td>180.0.10</td>
<td>533</td>
<td>0x80000099</td>
<td>0x3f1f</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>180.0.0.11</td>
<td>180.0.11</td>
<td>137</td>
<td>0x80000086</td>
<td>0xc58f</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>180.0.0.12</td>
<td>180.0.12</td>
<td>918</td>
<td>0x80000099</td>
<td>0x4cf3</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Router</td>
<td>180.0.0.13</td>
<td>180.0.13</td>
<td>1401</td>
<td>0x800000aa</td>
<td>0x879c</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Network</td>
<td>180.0.53.28</td>
<td>180.0.28</td>
<td>149</td>
<td>0x80000083</td>
<td>0xe5cd</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Network</td>
<td>180.0.54.28</td>
<td>180.0.28</td>
<td>1259</td>
<td>0x80000083</td>
<td>0x6d7</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Summary</td>
<td>180.0.0.15</td>
<td>180.0.10</td>
<td>376</td>
<td>0x80000084</td>
<td>0x6e1a</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Summary</td>
<td>180.0.0.15</td>
<td>180.0.12</td>
<td>73</td>
<td>0x80000084</td>
<td>0xd6ab</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Summary</td>
<td>180.0.0.18</td>
<td>180.0.10</td>
<td>1177</td>
<td>0x80000083</td>
<td>0xc6fb</td>
</tr>
<tr>
<td>0.0.0.1</td>
<td>Router</td>
<td>180.100.25.4</td>
<td>180.0.12</td>
<td>208</td>
<td>0x80000091</td>
<td>0x3049</td>
</tr>
<tr>
<td>0.0.0.1</td>
<td>AS Summ</td>
<td>180.0.0.9</td>
<td>180.0.10</td>
<td>824</td>
<td>0x80000084</td>
<td>0x3d07</td>
</tr>
<tr>
<td>0.0.0.1</td>
<td>AS Summ</td>
<td>180.0.0.9</td>
<td>180.0.12</td>
<td>1183</td>
<td>0x80000085</td>
<td>0x4bdf</td>
</tr>
<tr>
<td>0.0.0.1</td>
<td>AS Summ</td>
<td>180.0.0.8</td>
<td>180.0.10</td>
<td>244</td>
<td>0x80000082</td>
<td>0x73cb</td>
</tr>
<tr>
<td>n/a</td>
<td>AS Ext</td>
<td>7.1.0.0</td>
<td>180.0.23</td>
<td>1312</td>
<td>0x80000083</td>
<td>0x45e7</td>
</tr>
<tr>
<td>n/a</td>
<td>AS Ext</td>
<td>7.2.0.0</td>
<td>180.0.23</td>
<td>997</td>
<td>0x80000082</td>
<td>0x45e6</td>
</tr>
<tr>
<td>n/a</td>
<td>AS Ext</td>
<td>10.20.0.0</td>
<td>180.0.23</td>
<td>238</td>
<td>0x80000081</td>
<td>0x2d81</td>
</tr>
</tbody>
</table>

...  

No. of LSAs: 339
```

A:ALA-A#

A:ALA-A# `show router ospf database detail`

```
Router LSA for Area 0.0.0.0
```

---
<table>
<thead>
<tr>
<th>Area Id</th>
<th>0.0.0.0</th>
<th>Adv Router Id</th>
<th>180.0.0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link State Id</td>
<td>180.0.0.2</td>
<td>LSA Type</td>
<td>Router</td>
</tr>
<tr>
<td>Sequence No</td>
<td>0x88000000b7</td>
<td>Checksum</td>
<td>0xda55</td>
</tr>
<tr>
<td>Age</td>
<td>155</td>
<td>Length</td>
<td>192</td>
</tr>
<tr>
<td>Options</td>
<td>E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flags</td>
<td>None</td>
<td>Link Count</td>
<td>14</td>
</tr>
<tr>
<td>Link Type (1)</td>
<td>Point To Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nbr Rtr Id (1)</td>
<td>180.0.0.13</td>
<td>I/F Address (1)</td>
<td>180.0.22.2</td>
</tr>
<tr>
<td>No of TOS (1)</td>
<td>0</td>
<td>Metric-0 (1)</td>
<td>25</td>
</tr>
<tr>
<td>Link Type (2)</td>
<td>Stub Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (2)</td>
<td>180.0.22.0</td>
<td>Mask (2)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>No of TOS (2)</td>
<td>0</td>
<td>Metric-0 (2)</td>
<td>25</td>
</tr>
<tr>
<td>Link Type (3)</td>
<td>Point To Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nbr Rtr Id (3)</td>
<td>180.0.0.12</td>
<td>I/F Address (3)</td>
<td>180.0.5.2</td>
</tr>
<tr>
<td>No of TOS (3)</td>
<td>0</td>
<td>Metric-0 (3)</td>
<td>25</td>
</tr>
<tr>
<td>Link Type (4)</td>
<td>Stub Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (4)</td>
<td>180.0.5.0</td>
<td>Mask (4)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>No of TOS (4)</td>
<td>0</td>
<td>Metric-0 (4)</td>
<td>25</td>
</tr>
<tr>
<td>Link Type (5)</td>
<td>Point To Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nbr Rtr Id (5)</td>
<td>180.0.0.8</td>
<td>Mask (5)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>No of TOS (5)</td>
<td>0</td>
<td>Metric-0 (5)</td>
<td>6</td>
</tr>
<tr>
<td>Link Type (6)</td>
<td>Stub Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (6)</td>
<td>180.0.13.0</td>
<td>Mask (6)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>No of TOS (6)</td>
<td>0</td>
<td>Metric-0 (6)</td>
<td>6</td>
</tr>
<tr>
<td>Link Type (7)</td>
<td>Point To Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nbr Rtr Id (7)</td>
<td>180.0.0.5</td>
<td>I/F Address (7)</td>
<td>180.0.14.2</td>
</tr>
<tr>
<td>No of TOS (7)</td>
<td>0</td>
<td>Metric-0 (7)</td>
<td>6</td>
</tr>
<tr>
<td>Link Type (8)</td>
<td>Stub Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (8)</td>
<td>180.0.14.0</td>
<td>Mask (8)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>No of TOS (8)</td>
<td>0</td>
<td>Metric-0 (8)</td>
<td>6</td>
</tr>
<tr>
<td>Link Type (9)</td>
<td>Point To Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nbr Rtr Id (9)</td>
<td>180.0.0.11</td>
<td>I/F Address (9)</td>
<td>180.0.17.2</td>
</tr>
<tr>
<td>No of TOS (9)</td>
<td>0</td>
<td>Metric-0 (9)</td>
<td>25</td>
</tr>
<tr>
<td>Link Type (10)</td>
<td>Stub Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (10)</td>
<td>180.0.17.0</td>
<td>Mask (10)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>No of TOS (10)</td>
<td>0</td>
<td>Metric-0 (10)</td>
<td>25</td>
</tr>
<tr>
<td>Link Type (11)</td>
<td>Stub Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (11)</td>
<td>180.0.0.2</td>
<td>Mask (11)</td>
<td>255.255.255.255</td>
</tr>
<tr>
<td>No of TOS (11)</td>
<td>0</td>
<td>Metric-0 (11)</td>
<td>1</td>
</tr>
<tr>
<td>Link Type (12)</td>
<td>Stub Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (12)</td>
<td>180.0.18.0</td>
<td>Mask (12)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>No of TOS (12)</td>
<td>0</td>
<td>Metric-0 (12)</td>
<td>24</td>
</tr>
<tr>
<td>Link Type (13)</td>
<td>Point To Point</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nbr Rtr Id (13)</td>
<td>180.0.0.10</td>
<td>I/F Address (13)</td>
<td>180.0.3.2</td>
</tr>
<tr>
<td>No of TOS (13)</td>
<td>0</td>
<td>Metric-0 (13)</td>
<td>25</td>
</tr>
<tr>
<td>Link Type (14)</td>
<td>Stub Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network (14)</td>
<td>180.0.3.0</td>
<td>Mask (14)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>No of TOS (14)</td>
<td>0</td>
<td>Metric-0 (14)</td>
<td>25</td>
</tr>
</tbody>
</table>

---

**AS Ext LSA for Network 180.0.0.14**

<table>
<thead>
<tr>
<th>Area Id</th>
<th>N/A</th>
<th>Adv Router Id</th>
<th>180.0.0.10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link State Id</td>
<td>180.0.0.14</td>
<td>LSA Type</td>
<td>AS Ext</td>
</tr>
<tr>
<td>Sequence No</td>
<td>0x88000000083</td>
<td>Checksum</td>
<td>0xda659</td>
</tr>
<tr>
<td>Age</td>
<td>2033</td>
<td>Length</td>
<td>36</td>
</tr>
<tr>
<td>Options</td>
<td>E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Mask</td>
<td>255.255.255.255</td>
<td>Fwding Address</td>
<td>180.1.6.15</td>
</tr>
<tr>
<td>Metric Type</td>
<td>Type 2</td>
<td>Metric-0</td>
<td>4</td>
</tr>
</tbody>
</table>
interface

Syntax  interface [ip-addr | ip-int-name | area area-id] [detail]

Context  show>router>ospf

Description  Displays the details of the OSPF interface, this interface can be identified by ip-address or ip interface name. When neither is specified, all in-service interfaces are displayed.

The detail option produces a great amount of data. It is recommended to detail only when requesting a specific interface.

Parameters  
ip-addr — Display only the interface identified by this IP address.
ip-int-name — Display only the interface identified by this interface name.
area area-id — Display all interfaces configured in this area.
detail — Displays detailed information on the interface.

Output  Standard OSPF Interface Output — The following table describes the standard command output fields for an OSPF interface.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Name</td>
<td>The interface name.</td>
</tr>
<tr>
<td>Area Id</td>
<td>A 32-bit integer uniquely identifying the area to which this interface is connected. Area ID 0.0.0.0 is used for the OSPF backbone.</td>
</tr>
<tr>
<td>D Rtr Id</td>
<td>The IP Interface address of the router identified as the Designated Router for the network in which this interface is configured. Set to 0.0.0.0 if there is no Designated router.</td>
</tr>
<tr>
<td>BD Rtr Id</td>
<td>The IP Interface address of the router identified as the Backup Designated Router for the network in which this interface is configured. Set to 0.0.0.0 if there is no Backup Designated router.</td>
</tr>
<tr>
<td>Adm</td>
<td>Dn  — OSPF on this interface is administratively shut down.</td>
</tr>
<tr>
<td></td>
<td>Up  — OSPF on this interface is administratively enabled.</td>
</tr>
<tr>
<td>Opr</td>
<td>Down — This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable.</td>
</tr>
<tr>
<td></td>
<td>Wait — The router is trying to determine the identity of the (Backup) Designated router for the network.</td>
</tr>
</tbody>
</table>
Show Commands

**Sample Output**

A:SetupCLI# show router ospf interface "ip_if_1" detail

```
OSPF Interface (Detailed) : ip_if_1

Configuration

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PToP</td>
<td>The interface is operational, and connects either to a physical point-to-point network or to a virtual link.</td>
</tr>
<tr>
<td>DR</td>
<td>This router is the Designated Router for this network.</td>
</tr>
<tr>
<td>BDR</td>
<td>This router is the backup Designated Router for this network.</td>
</tr>
<tr>
<td>ODR</td>
<td>The interface is operational and part of a broadcast or NBMA network on which another router has been selected to be the Designated Router.</td>
</tr>
</tbody>
</table>

No. of OSPF Interfaces

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The number of interfaces listed.</td>
</tr>
</tbody>
</table>

Sample Output

A:SetupCLI# show router ospf interface "ip_if_1" detail

```

OSPF Interface (Detailed) : ip_if_1

Configuration

- IP Address : 10.10.1.1
- Area Id : 0.0.0.0
- Hello Intrvl : 9 sec
- Retrans Intrvl : 10 sec
- Cfg Metric : 11
- Transit Delay : 2
- Passive : False
- LFA : Exclude
- IPsec InStatSA : 
- IPsec OutStatSA :
- IPsec InStatSATmp :

State

- Admin Status : Enabled
- Designated Rtr : 0.0.0.0
- IF Type : Secondary
- Oper MTU : 1576
- Oper Metric : 11
- Te Metric : 16777215
- Admin Groups : None
- Ldp Sync : outOfService
- Ldp Tm Left : 0

Statistics

- Nbr Count : 0
- Tot Rx Packets : 0
- Rx Hellos : 0
- Rx DBDs : 0
- Rx LSRs : 0
- Rx LS Ack : 0
- If Events : 0
- Tot Tx Packets : 0
- Tx Hellos : 0
- Tx DBDs : 0
- Tx LSRs : 0
- Tx LS Ack : 0
- Ldp Sync Wait : Disabled
- Ldp Tm Left : 0

PToP — The interface is operational, and connects either to a physical point-to-point network or to a virtual link.

DR — This router is the Designated Router for this network.

BDR — This router is the backup Designated Router for this network.

ODR — The interface is operational and part of a broadcast or NBMA network on which another router has been selected to be the Designated Router.

No. of OSPF Interfaces

The number of interfaces listed.
Retransmits : 0      Discards : 0
Bad Networks : 0      Bad Virt Links : 0
Bad Areas : 0      Bad Dest Addr : 0
Bad Auth Types : 0      Auth Failures : 0
Bad Neighbors : 0      Bad Pkt Types : 0
Bad Lengths : 0      Bad Hello Int. : 0
Bad Dead Int. : 0      Bad Options : 0
Bad Versions : 0      Bad Checksums : 0
LSA Count : 0      LSA Checksum : 0x0
-------------------------------------------------------------------------------
Configuration
-------------------------------------------------------------------------------
IP Address : 10.10.1.1
Area Id : 1.1.1.1      Priority : 10
Hello Intrvl : 9 sec      Rtr Dead Intrvl : 45 sec
Retrans Intrvl : 10 sec      Poll Intrvl : 120 sec
Cfg Metric : 11      Advert Subnet : False
Transit Delay : 2      Auth Type : MD5
Passive : False      Cfg MTU : 9198
LFA : Exclude
IPsec InStatSA :  IPsec OutStatSA :
IPsec InStatSATmp :
-------------------------------------------------------------------------------
State
-------------------------------------------------------------------------------
Admin Status : Enabled      Oper State : Down
Designated Rtr : 0.0.0.0      Backup Desig Rtr : 0.0.0.0
IF Type : Point To Point      Network Type : Stub
Oper MTU : 1576      Last Enabled : Never
Oper Metric : 11      Bfd Enabled : No
Te Metric : 16777215      Te State : Down
Admin Groups : None
Ldp Sync : outOfService      Ldp Sync Wait : Disabled
Ldp Timer State : Disabled      Ldp Tm Left : 0
-------------------------------------------------------------------------------
Statistics
-------------------------------------------------------------------------------
Nbr Count : 0      If Events : 0
Tot Rx Packets : 0      Tot Tx Packets : 0
Rx Hellos : 0      Tx Hellos : 0
Rx DBDs : 0      Tx DBDs : 0
Rx LSRs : 0      Tx LSRs : 0
Rx LSUs : 0      Tx LSUs : 0
Rx LS Acks : 0      Tx LS Acks : 0
Retransmits : 0      Discards : 0
Bad Networks : 0      Bad Virt Links : 0
Bad Areas : 0      Bad Dest Addr : 0
Bad Auth Types : 0      Auth Failures : 0
Bad Neighbors : 0      Bad Pkt Types : 0
Bad Lengths : 0      Bad Hello Int. : 0
Bad Dead Int. : 0      Bad Options : 0
Bad Versions : 0      Bad Checksums : 0
LSA Count : 0      LSA Checksum : 0x0
-------------------------------------------------------------------------------
A:SetupCLI#

A:SetupCLI# show router ospf interface area 1.1.1.1 detail
-------------------------------------------------------------------------------
OSPF Interfaces in Area (Detailed) : 1.1.1.1
===============================================================================
Interface : ip_if_1
===============================================================================
IP Address       : 10.10.1.1
Area Id          : 1.1.1.1              Priority         : 10
Hello Intrvl     : 9 sec                Rtr Dead Intrvl  : 45 sec
Retrans Intrvl   : 10 sec               Poll Intrvl      : 120 sec
Cfg Metric       : 11                    Advert Subnet    : False
Transit Delay    : 2                     Auth Type        : MD5
Passive          : False                  Cfg MTU          : 9198
LFA              : Exclude
IPsec InStatSA   :                      IPsec OutStatSA  :
IPsec InStatSATmp:
Admin Status     : Enabled              Oper State       : Down
Designated Rtr   : 0.0.0.0              Backup Desig Rtr : 0.0.0.0
IF Type          : Point To Point       Network Type     : Stub
Oper MTU         : 1576                  Last Enabled     : Never
Oper Metric      : 11                    Bfd Enabled      : No
Te Metric        : 16777215              Te State         : Down
Admin Groups     : None                   If Events        : 0
Ldp Sync         : outOfService         Ldp Sync Wait    : Disabled
Ldp Timer State  : Disabled             Ldp Tm Left      : 0
Nbr Count        : 0                     If Events        : 0
Tot Rx Packets   : 0                    Tot Tx Packets   : 0
Rx Hellos        : 0                    Tx Hellos        : 0
Rx DBDs          : 0                    Tx DBDs          : 0
Rx LSRs          : 0                    Tx LSRs          : 0
Rx LSUs          : 0                    Tx LSUs          : 0
Rx LS Acks       : 0                    Tx LS Acks       : 0
Retransmits      : 0                    Discards         : 0
Bad Networks     : 0                    Bad Virt Links   : 0
Bad Areas        : 0                    Bad Dest Addr    : 0
Bad Auth Types   : 0                    Auth Failures    : 0
Bad Neighbors    : 0                    Bad Pkt Types    : 0
Bad Lengths      : 0                    Bad Hello Int.   : 0
Bad Dead Int.    : 0                    Bad Options      : 0
Bad Versions     : 0                    Bad Checksums    : 0
LSA Count        : 0                    LSA Checksum     : 0x0
===============================================================================
A:SetupCLI#
A:SetupCLI# show router ospf 1 interface detail
===============================================================================
OSPF Interfaces (Detailed)
-------------------------------------------------------------------------------
Interface : system
-------------------------------------------------------------------------------
IP Address       : 9.1.255.255
Area Id          : 0.0.0.0              Priority         : 1
Hello Intrvl     : 10 sec               Rtr Dead Intrvl  : 40 sec
Retrans Intrvl   : 5 sec                Poll Intrvl      : 120 sec
Cfg Metric       : 0                    Advert Subnet    : True
Transit Delay    : 1                     Auth Type        : None
Passive          : True                  Cfg MTU          : 0
Admin Status     : Enabled              Oper State       : Designated Rtr
Designated Rtr   : 2.2.2.2               Backup Desig Rtr : 0.0.0.0
===============================================================================
A:SetupCLI#
The following table describes the detailed command output fields for an OSPF interface.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The IP address of this OSPF interface.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address and mask of this OSPF interface.</td>
</tr>
<tr>
<td>Interface Name</td>
<td>The interface name.</td>
</tr>
<tr>
<td>Area Id</td>
<td>A 32-bit integer uniquely identifying the area to which this interface is connected. Area ID 0.0.0.0 is used for the OSPF backbone.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of this interface. Used in multi-access networks, this field is used in the designated router election algorithm.</td>
</tr>
<tr>
<td>Hello Intrvl</td>
<td>The length of time, in seconds, between the Hello packets that the router sends on the interface. This value must be the same for all routers attached to a common network.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rtr Dead Intrvl</td>
<td>The number of seconds that a router’s Hello packets have not been seen before it’s neighbors declare the router down. This should be some multiple of the Hello interval. This value must be the same for all routers attached to a common network.</td>
</tr>
<tr>
<td>Retrans Intrvl</td>
<td>The number of seconds between link-state advertisement retransmissions, for adjacencies belonging to this interface. This value is also used when retransmitting database description and link-state request packets.</td>
</tr>
<tr>
<td>Poll Intrvl</td>
<td>The larger time interval, in seconds, between the Hello packets sent to an inactive non-broadcast multi-access neighbor.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric to be advertised for this interface.</td>
</tr>
<tr>
<td>Advert Subnet</td>
<td>False — When a point-to-point interface is configured as false, then the subnet is not advertised and the endpoints are advertised as host routes.</td>
</tr>
<tr>
<td></td>
<td>True — When a point-to-point interface is configured to true, then the subnet is advertised.</td>
</tr>
<tr>
<td>Transit Delay</td>
<td>The estimated number of seconds it takes to transmit a link state update packet over this interface.</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Identifies the authentication procedure to be used for the packet.</td>
</tr>
<tr>
<td></td>
<td>None — Routing exchanges over the network/subnet are not authenticated.</td>
</tr>
<tr>
<td></td>
<td>Simple — A 64-bit field is configured on a per-network basis. All packets sent on a particular network must have this configured value in their OSPF header 64-bit authentication field. This essentially serves as a “clear” 64-bit password.</td>
</tr>
<tr>
<td></td>
<td>MD5 — A shared secret key is configured in all routers attached to a common network/subnet. For each OSPF protocol packet, the key is used to generate/verify a “message digest” that is appended to the end of the OSPF packet.</td>
</tr>
<tr>
<td>Passive</td>
<td>False — This interfaces operates as a normal OSPF interface with regard to adjacency forming and network/link behavior.</td>
</tr>
<tr>
<td></td>
<td>True — no OSPF HELLOs will be sent out on this interface and the router advertises this interface as a stub network/link in its router LSAs.</td>
</tr>
<tr>
<td>MTU</td>
<td>The desired size of the largest packet which can be sent/received on this OSPF interface, specified in octets. This size DOES include the underlying IP header length, but not the underlying layer headers/trailers.</td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Admin Status</td>
<td>Disabled – OSPF on this interface is administratively shut down.</td>
</tr>
<tr>
<td></td>
<td>Enabled – OSPF on this interface is administratively enabled.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Down – This is the initial interface state. In this state, the lower-level protocols have indicated that the interface is unusable.</td>
</tr>
<tr>
<td></td>
<td>Waiting – The router is trying to determine the identity of the (Backup) Designated router for the network.</td>
</tr>
<tr>
<td></td>
<td>Point To Point – The interface is operational, and connects either to a physical point-to-point network or to a virtual link.</td>
</tr>
<tr>
<td></td>
<td>Designated Rtr – This router is the Designated Router for this network.</td>
</tr>
<tr>
<td></td>
<td>Other Desig Rtr – The interface is operational and part of a broadcast or NBMA network on which another router has been selected to be the Designated Router.</td>
</tr>
<tr>
<td></td>
<td>Backup Desig Rtr – This router is the Backup Designated Router for this network.</td>
</tr>
<tr>
<td>DR-Id</td>
<td>The IP Interface address of the router identified as the Designated Router for the network in which this interface is configured. Set to 0.0.0.0 if there is no Designated router</td>
</tr>
<tr>
<td>BDR-Id</td>
<td>The IP Interface address of the router identified as the Backup Designated Router for the network in which this interface is configured. Set to 0.0.0.0 if there is no Backup Designated router</td>
</tr>
<tr>
<td>IF Type</td>
<td>Broadcast – LANs, such as Ethernet.</td>
</tr>
<tr>
<td></td>
<td>NBMA – X.25, Frame Relay and similar technologies.</td>
</tr>
<tr>
<td></td>
<td>Point-To-Point – Links that are definitively point to point.</td>
</tr>
<tr>
<td>Network Type</td>
<td>Stub – OSPF has not established a neighbor relationship with any other OSPF router on this network as such only traffic sourced or destined to this network will be routed to this network.</td>
</tr>
<tr>
<td></td>
<td>Transit – OSPF has established at least one neighbor relationship with any other OSPF router on this network as such traffic en route to other networks may be routed via this network.</td>
</tr>
<tr>
<td>Oper MTU</td>
<td>The operational size of the largest packet which can be sent/received on this OSPF interface, specified in octets. This size DOES include the underlying IP header length, but not the underlying layer headers/trailers.</td>
</tr>
<tr>
<td>Last Enabled</td>
<td>The time that this interface was last enabled to run OSPF on this interface.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>The number of OSPF neighbors on the network for this interface.</td>
</tr>
<tr>
<td>If Events</td>
<td>The number of times this OSPF interface has changed its state, or an error has occurred since this interface was last enabled.</td>
</tr>
<tr>
<td>Tot Rx Packets</td>
<td>The total number of OSPF packets received on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Tot Tx Packets</td>
<td>The total number of OSPF packets transmitted on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Rx Hellos</td>
<td>The total number of OSPF Hello packets received on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Tx Hellos</td>
<td>The total number of OSPF Hello packets transmitted on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Rx DBDs</td>
<td>The total number of OSPF database description packets received on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Tx DBDs</td>
<td>The total number of OSPF database description packets transmitted on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Rx LSRs</td>
<td>The total number of Link State Requests (LSRs) received on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Tx LSRs</td>
<td>The total number of Link State Requests (LSRs) transmitted on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Rx LSUs</td>
<td>The total number of Link State Updates (LSUs) received on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Tx LSUs</td>
<td>The total number of Link State Updates (LSUs) transmitted on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Rx LS Acks</td>
<td>The total number of Link State Acknowledgements received on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Tx LS Acks</td>
<td>The total number of Link State Acknowledgements transmitted on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Retransmits</td>
<td>The total number of OSPF Retransmits sent on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Discards</td>
<td>The total number of OSPF packets discarded on this interface since this interface was last enabled.</td>
</tr>
<tr>
<td>Bad Networks</td>
<td>The total number of OSPF packets received with invalid network or mask since this interface was last enabled.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Bad Virt Links</td>
<td>The total number of OSPF packets received on this interface that are</td>
</tr>
<tr>
<td></td>
<td>destined to a virtual link that does not exist since this interface was</td>
</tr>
<tr>
<td></td>
<td>last enabled.</td>
</tr>
<tr>
<td>Bad Areas</td>
<td>The total number of OSPF packets received with an area mismatch since this</td>
</tr>
<tr>
<td></td>
<td>interface was last enabled.</td>
</tr>
<tr>
<td>Bad Dest Addr</td>
<td>The total number of OSPF packets received with the incorrect IP destination</td>
</tr>
<tr>
<td></td>
<td>address since this interface was last enabled.</td>
</tr>
<tr>
<td>Bad Auth Types</td>
<td>The total number of OSPF packets received with an invalid authorization</td>
</tr>
<tr>
<td></td>
<td>type since this interface was last enabled.</td>
</tr>
<tr>
<td>Auth Failures</td>
<td>The total number of OSPF packets received with an invalid authorization</td>
</tr>
<tr>
<td></td>
<td>key since this interface was last enabled.</td>
</tr>
<tr>
<td>Bad Neighbors</td>
<td>The total number of OSPF packets received where the neighbor information</td>
</tr>
<tr>
<td></td>
<td>does not match the information this router has for the neighbor since this</td>
</tr>
<tr>
<td></td>
<td>interface was last enabled.</td>
</tr>
<tr>
<td>Bad Pkt Types</td>
<td>The total number of OSPF packets received with an invalid OSPF packet type</td>
</tr>
<tr>
<td></td>
<td>since this interface was last enabled.</td>
</tr>
<tr>
<td>Bad Lengths</td>
<td>The total number of OSPF packets received on this interface with a total</td>
</tr>
<tr>
<td></td>
<td>length not equal to the length given in the packet itself since this</td>
</tr>
<tr>
<td></td>
<td>interface was last enabled.</td>
</tr>
<tr>
<td>Bad Hello int.</td>
<td>The total number of OSPF packets received where the hello interval given</td>
</tr>
<tr>
<td></td>
<td>in packet was not equal to that configured on this interface since this</td>
</tr>
<tr>
<td></td>
<td>interface was last enabled.</td>
</tr>
<tr>
<td>Bad Dead Int.</td>
<td>The total number of OSPF packets received where the dead interval given in</td>
</tr>
<tr>
<td></td>
<td>the packet was not equal to that configured on this interface since this</td>
</tr>
<tr>
<td></td>
<td>interface was last enabled.</td>
</tr>
<tr>
<td>Bad Options</td>
<td>The total number of OSPF packets received with an option that does not</td>
</tr>
<tr>
<td></td>
<td>match those configured for this interface or area since this interface was</td>
</tr>
<tr>
<td></td>
<td>last enabled.</td>
</tr>
<tr>
<td>Bad Versions</td>
<td>The total number of OSPF packets received with bad OSPF version numbers</td>
</tr>
<tr>
<td></td>
<td>since this interface was last enabled.</td>
</tr>
<tr>
<td>Te Metric</td>
<td>Indicates the TE metric configured for this interface. This metric is</td>
</tr>
<tr>
<td></td>
<td>flooded out in the TE metric sub-tlv in the OSPF TE LSAs. Depending on the</td>
</tr>
<tr>
<td></td>
<td>configuration, either the TE metric value or the native OSPF metric value</td>
</tr>
<tr>
<td></td>
<td>is used in CSPF computations.</td>
</tr>
<tr>
<td>Te State</td>
<td>Indicates the MPLS interface TE status from OSPF standpoint.</td>
</tr>
<tr>
<td>Admin Groups</td>
<td>Indicates the bit-map inherited from MPLS interface that identifies the</td>
</tr>
<tr>
<td></td>
<td>admin groups to which this interface belongs.</td>
</tr>
</tbody>
</table>
Show Commands

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ldp Sync</td>
<td>Specifies whether the IGP-LDP synchronization feature is enabled or disabled on all interfaces participating in the OSPF routing protocol.</td>
</tr>
<tr>
<td>Ldp Sync Wait</td>
<td>Indicates the time to wait for the LDP adjacency to come up.</td>
</tr>
<tr>
<td>Ldp Timer State</td>
<td>Indicates the state of the LDP sync time left on the OSPF interface.</td>
</tr>
<tr>
<td>Ldp Tm Left</td>
<td>Indicates the time left before OSPF reverts back to advertising normal metric for this interface.</td>
</tr>
</tbody>
</table>

Sample Output

*A:JC-NodeA# show router ospf interface area 1 detail

OSPF Interfaces in Area (Detailed) : 1

Interface : ip-10.10.1.1

IP Address       : 10.10.1.1
Area Id          : 0.0.0.1              Priority         : 1
Hello Intrvl     : 5 sec                Rtr Dead Intrvl  : 15 sec
Retrans Intrvl   : 5 sec                Poll Intrvl      : 120 sec
Cfg Metric       : 0                    Advert Subnet    : True
Transit Delay    : 1                    Auth Type        : None
Passive          : False                Cfg MTU          : 0
Admin Status     : Enabled              Oper State       : Designated Rtr
Designated Rtr   : 10.20.1.1            Backup Desig Rtr : 0.0.0.0
IF Type          : Broadcast            Network Type     : Transit
Oper MTU         : 1500                 Last Enabled     : 04/11/2007 16:06:27
Oper Metric      : 1000                 Bfd Enabled      : No
Nbr Count        : 0                    If Events        : 5
Tot Rx Packets   : 0                    Tot Tx Packets   : 1116
Rx Hellos        : 0                    Tx Hellos        : 1116
Rx DBDs          : 0                    Tx DBDs          : 0
Rx LSRs          : 0                    Tx LSRs          : 0
Rx LSUs          : 0                    Tx LSUs          : 0
Rx LS Acks       : 0                    Tx LS Acks       : 0
Retransmits      : 0                    Discards         : 0
Bad Networks     : 0                    Bad Virt Links   : 0
Bad Areas        : 0                    Bad Dest Addr    : 0
Bad Auth Types   : 0                    Auth Failures    : 0
Bad Neighbors    : 0                    Bad Pkt Types    : 0
Bad Lengths      : 0                    Bad Hello Int.   : 0
Bad Dead Int.    : 0                    Bad Options      : 0
Bad Versions     : 0                    Bad Checksums    : 0
LSA Count        : 0                    LSA Checksum     : 0x0
TE Metric        : 678

*A:JC-NodeA#
### Ifa-coverage

**Syntax**   
Ifa-coverage

**Context**  
show>router>ospf

**Description**  
This command displays OSPF Loop-Free Alternate (LFA) next-hop information.

**Sample Output**

```
*A:Dut-A# show router ospf ifa-coverage
=======================================================================
LFA coverage ospfv2 instance 0
=======================================================================
<table>
<thead>
<tr>
<th>Area</th>
<th>Node</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>4/4(100%)</td>
<td>8/8(100%)</td>
</tr>
</tbody>
</table>
=======================================================================
*A:Dut-A#
```

### neighbor

**Syntax**   
neighbor [ip-int-name] [router-id]

**Context**  
show>router>ospf

**Description**  
This command will display all neighbor information. To reduce the amount of output the user may opt to select the neighbors on a given interface by address or name.

The **detail** option produces a large amount of data. It is recommended to use **detail** only when requesting a specific neighbor.

**Parameters**

- **ip-int-name** — Display neighbor information only for neighbors of the interface identified by the interface name
- **router-id** — Display neighbor information for the neighbor identified by the specified router ID.

**Output**

**Standard OSPF Neighbor Output** — The following table describes the standard command output fields for an OSPF neighbor.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nbr IP Addr</td>
<td>The IP address this neighbor is using in its IP Source Address. Note that, on addressless links, this will not be 0.0.0.0, but the address of another of the neighbor's interfaces.</td>
</tr>
<tr>
<td>Nbr Rtr Id</td>
<td>A 32-bit integer uniquely identifying the neighboring router in the Autonomous System.</td>
</tr>
<tr>
<td>Nbr State</td>
<td><strong>Down</strong> — This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor.</td>
</tr>
</tbody>
</table>
Sample Output

A:ALA-A# show router ospf 1 neighbor

<table>
<thead>
<tr>
<th>Interface-Name</th>
<th>Rtr Id</th>
<th>State</th>
<th>Pri</th>
<th>RetxQ</th>
<th>TTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>pc157-2/1</td>
<td>10.13.8.158</td>
<td>Full</td>
<td>1</td>
<td>0</td>
<td>37</td>
</tr>
<tr>
<td>pc157-2/2</td>
<td>10.13.7.165</td>
<td>Full</td>
<td>100</td>
<td>0</td>
<td>33</td>
</tr>
<tr>
<td>pc157-2/3</td>
<td>10.13.6.188</td>
<td>Full</td>
<td>1</td>
<td>0</td>
<td>38</td>
</tr>
</tbody>
</table>

Attempt — This state is only valid for neighbors attached to NBMA networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor.

Init — In this state, an Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet).

Two Way — In this state, communication between the two routers is bidirectional.

ExchStart — This is 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 Descriptor sequence number.

Exchange — In this state the router is describing its entire link state database by sending Database Description packets to the neighbor.

Loading — In this state, Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.

Full — In this state, the neighboring routers are fully adjacent. These adjacencies will now appear in router-LSAs and network-LSAs.

Priority
The priority of this neighbor in the designated router election algorithm. The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network.

RetxQ Len
The current length of the retransmission queue.

Dead Time
The time until this neighbor is declared down, this timer is set to the dead router interval when a valid hello packet is received from the neighbor.

No. of Neighbors
The number of adjacent OSPF neighbors on this interface.
No. of Neighbors: 3

A:ALA-A#

### Detailed OSPF Neighbor Output

The following table describes the detailed command output fields for an OSPF neighbor.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor IP Addr</td>
<td>The IP address this neighbor is using in its IP source address. Note that, on addressless links, this will not be 0.0.0.0, but the address of another of the neighbor's interfaces.</td>
</tr>
<tr>
<td>Local IF IP Addr</td>
<td>The IP address of this OSPF interface.</td>
</tr>
<tr>
<td>Area Id</td>
<td>A 32-bit integer uniquely identifying the area to which this interface is connected. Area ID 0.0.0.0 is used for the OSPF backbone.</td>
</tr>
<tr>
<td>Designated Rtr</td>
<td>The IP Interface address of the router identified as the Designated Router for the network in which this interface is configured. Set to 0.0.0.0 if there is no Designated router.</td>
</tr>
<tr>
<td>Neighbor Rtr Id</td>
<td>A 32-bit integer uniquely identifying the neighboring router in the AS.</td>
</tr>
<tr>
<td>Neighbor State</td>
<td><strong>Down</strong> — This is the initial state of a neighbor conversation. It indicates that there has been no recent information received from the neighbor.</td>
</tr>
<tr>
<td></td>
<td><strong>Attempt</strong> — This state is only valid for neighbors attached to NBMA networks. It indicates that no recent information has been received from the neighbor, but that a more concerted effort should be made to contact the neighbor.</td>
</tr>
<tr>
<td></td>
<td><strong>Init</strong> — In this state, an Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor (i.e., the router itself did not appear in the neighbor's Hello packet).</td>
</tr>
<tr>
<td></td>
<td><strong>Two Way</strong> — In this state, communication between the two routers is bidirectional.</td>
</tr>
<tr>
<td></td>
<td><strong>Exchange start</strong> — This is 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 Descriptor sequence number.</td>
</tr>
<tr>
<td></td>
<td><strong>Exchange</strong> — In this state the router is describing its entire link state database by sending Database Description packets to the neighbor.</td>
</tr>
<tr>
<td></td>
<td><strong>Loading</strong> — In this state, Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Full</td>
<td>In this state, the neighboring routers are fully adjacent. These adjacencies will now appear in router-LSAs and network-LSAs.</td>
</tr>
<tr>
<td>Priority</td>
<td>The priority of this neighbor in the designated router election algorithm. The value 0 signifies that the neighbor is not eligible to become the designated router on this particular network.</td>
</tr>
<tr>
<td>Retrans Q Length</td>
<td>The current length of the retransmission queue.</td>
</tr>
</tbody>
</table>
| Options          | E – External Routes Support  
|                  | MC – Multicast Support  
|                  | N/P – Type 7 LSA Support  
|                  | EA – External Attribute LSA Support  
|                  | DC – Demand Circuit Support  
|                  | O – Opaque LSA Support                                                   |
| Backup Desig Rtr | The IP Interface address of the router identified as the Backup Designated Router for the network in which this interface is configured. Set to 0.0.0.0 if there is no backup designated router. |
| Events           | The number of times this neighbor relationship has changed state, or an error has occurred. |
| Last Event Time  | The time when the last event occurred that affected the adjacency to the neighbor. |
| Up Time          | This value represents the uninterrupted time, in hundredths of seconds, the adjacency to this neighbor has been up. To evaluate when the last state change occurred see last event time. |
| Time Before Dead | The time until this neighbor is declared down, this timer is set to the dead router interval when a valid hello packet is received from the neighbor. |
| Bad Nbr States   | The total number of OSPF packets received when the neighbor state was not expecting to receive this packet type since this interface was last enabled. |
| LSA Inst fails   | The total number of times an LSA could not be installed into the LSDB due to a resource allocation issue since this interface was last enabled. |
| Bad Seq Nums     | The total number of times when a database description packet was received with a sequence number mismatch since this interface was last enabled. |
| Bad MTUs         | The total number of times when the MTU in a received database description packet was larger than the MTU of the receiving interface since this interface was last enabled. |
**Sample Output**

A:ALA-A# `show router ospf neighbor detail`

```
OSPF Neighbors

Neighbor Rtr Id    : 10.13.8.158    Interface: pc157-2/1
Neighbor IP Addr   : 10.16.1.8
Local IF IP Addr  : 10.16.1.7
Area Id           : 0.0.0.0
Designated Rtr    : 0.0.0.0    Backup Desig Rtr : 0.0.0.0
Neighbor State    : Full
Retrans Q Length  : 0
Events            : 4
Up Time           : 1d 18:20:20
GR Helper         : Not Helping
GR Exit Reason    : None
Bad Nbr States    : 1
Bad Seq Nums      : 0
Bad Packets       : 0
Option Mismatches : 0
Num Restarts      : 0
LSA not in LSDB   : 0
Bad Nbr States    : 0
LSA Inst fails    : 0
Bad Seq Nums      : 0
Bad Packets       : 0
Option Mismatches : 0
LSA not in LSDB   : 0
Bad Nbr States    : 0
LSA Inst fails    : 0
Bad Seq Nums      : 0
Bad Packets       : 0
Option Mismatches : 0
LSA not in LSDB   : 0

Neighbor Rtr Id    : 10.13.7.165    Interface: pc157-2/2
Neighbor IP Addr   : 10.12.1.3
Local IF IP Addr  : 10.12.1.7
Area Id           : 0.0.0.0
Designated Rtr    : 0.0.0.0    Backup Desig Rtr : 10.13.9.157
Neighbor State    : Full    Priority     : 100
Retrans Q Length  : 0
Events            : 4
Up Time           : 0d 16:52:27
GR Helper         : Not Helping
GR Exit Reason    : None
Bad Nbr States    : 0
LSA Inst fails    : 0
Bad Seq Nums      : 0
Bad MTUs          : 0
```

**Label** | **Description (Continued)**
---|---
Bad Packets | The total number of times when an LS update was received with an illegal LS type or an option mismatch since this interface was last enabled.
LSA not in LSDB | The total number of times when an LS request was received for an LSA not installed in the LSDB of this router since this interface was last enabled.
Option Mismatches | The total number of times when a LS update was received with an option mismatch since this interface was last enabled.
Nbr Duplicates | The total number of times when a duplicate database description packet was received during the exchange state since this interface was last enabled.
opaque-database

Syntax opaque-database [link link-id | area area-id | as] [adv-router router-id] [ls-id] [detail]

Context show>router>ospf

Description This command displays OSPF opaque database information.

Output OSPF Opaque Database Output — The following table describes the OSPF opaque database output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Id</td>
<td>A 32-bit integer uniquely identifying an area. Area ID 0.0.0.0 is used for the OSPF backbone.</td>
</tr>
<tr>
<td>Type</td>
<td>NSSA — This area is configured as a NSSA area.</td>
</tr>
<tr>
<td></td>
<td>Area — This area is configured as a standard area (not NSSA or stub).</td>
</tr>
<tr>
<td></td>
<td>Stub — This area is configured as a NSSA area.</td>
</tr>
<tr>
<td>Link State Id</td>
<td>The link state ID is an LSA type specific field containing either a Router-Id or an IP Address; it identifies the piece of the routing domain being described by the advertisement.</td>
</tr>
<tr>
<td>Adv Rtr Id</td>
<td>The router identifier of the router advertising the LSA.</td>
</tr>
<tr>
<td>Age</td>
<td>The age of the link state advertisement in seconds.</td>
</tr>
</tbody>
</table>
### Sample Output

**A:ALA-A#** show router ospf opaque-database

<table>
<thead>
<tr>
<th>Area Id</th>
<th>Type</th>
<th>Link State Id</th>
<th>Adv Rtr Id</th>
<th>Age</th>
<th>Sequence</th>
<th>Cksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.0.2</td>
<td>205</td>
<td>0x8000007e</td>
<td>0xb1b2</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.0.5</td>
<td>617</td>
<td>0x80000084</td>
<td>0xb1a6</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.0.8</td>
<td>1635</td>
<td>0x80000081</td>
<td>0xc391</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.0.9</td>
<td>1306</td>
<td>0x80000082</td>
<td>0xc58c</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.10</td>
<td>53</td>
<td>0x80000082</td>
<td>0xc986</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.11</td>
<td>577</td>
<td>0x8000007e</td>
<td>0xd57c</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.12</td>
<td>1628</td>
<td>0x80000080</td>
<td>0xd578</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.13</td>
<td>581</td>
<td>0x80000080</td>
<td>0xd972</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.22</td>
<td>1006</td>
<td>0x80000080</td>
<td>0xfd3c</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.23</td>
<td>1238</td>
<td>0x80000083</td>
<td>0xfb39</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.27</td>
<td>55</td>
<td>0x80000083</td>
<td>0xc21</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.28</td>
<td>389</td>
<td>0x80000083</td>
<td>0x101b</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.29</td>
<td>1658</td>
<td>0x80000082</td>
<td>0xe16d</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.1</td>
<td>180.0.30</td>
<td>976</td>
<td>0x80000083</td>
<td>0x180f</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.2</td>
<td>180.0.0.2</td>
<td>45</td>
<td>0x80000080</td>
<td>0x2f60</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.2</td>
<td>180.0.0.5</td>
<td>1357</td>
<td>0x80000084</td>
<td>0x7038</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>Area</td>
<td>1.0.0.2</td>
<td>180.0.0.8</td>
<td>1960</td>
<td>0x80000084</td>
<td>0x3472</td>
</tr>
</tbody>
</table>

---

No. of Opaque LSAs: 88

**A:ALA-A#**

*A:Dut-A#* show router ospf opaque-database adv-router 10.20.1.1 detail

<table>
<thead>
<tr>
<th>Area Id</th>
<th>Adv Router Id</th>
<th>LSA Type</th>
<th>Sequence No</th>
<th>Checksum</th>
<th>Age</th>
<th>Length</th>
<th>Options</th>
<th>Advertisement</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>10.20.1.1</td>
<td>Area Opaque</td>
<td>0x80000028</td>
<td>0xb136</td>
<td>192</td>
<td>28</td>
<td>E</td>
<td>ROUTER-ID TLV (0001) Len 4: 10.20.1.1</td>
</tr>
</tbody>
</table>

---

**A:ALA-A#**
Show Commands

**Link State Id**: 1.0.0.2  
**LSA Type**: Area Opaque  
**Sequence No**: 0x8000000d  
**Checksum**: 0x17f3  
**Age**: 678  
**Length**: 164  
**Options**: E  
**Advertisement**:

```
LINK INFO TLV (0002) Len 140 :
Sub-TLV: 1 Len: 1 LINK_TYPE : 2
Sub-TLV: 2 Len: 4 LINK_ID : 10.10.1.2
Sub-TLV: 3 Len: 4 LOC_IP_ADDR : 10.10.1.1
Sub-TLV: 4 Len: 4 REM_IP_ADDR : 0.0.0.0
Sub-TLV: 5 Len: 4 TE_METRIC : 1000
Sub-TLV: 6 Len: 4 MAX_BDWTH : 100000 Kbps
Sub-TLV: 7 Len: 4 RSRVBL_BDWTH : 800000 Kbps
Sub-TLV: 8 Len: 32 UNRsrvd_CLS0 :
  P0: 80000 Kbps P1: 320000 Kbps P2: 320000 Kbps P3: 320000 Kbps
Sub-TLV: 9 Len: 4 ADMIN_GROUP : 0 None
Sub-TLV: 17 Len: 36 TELK_BW_CONST:
  BW Model : MAM
  BC0: 80000 Kbps BC1: 0 Kbps BC2: 320000 Kbps BC3: 0 Kbps
  BC4: 0 Kbps BC5: 400000 Kbps BC6: 0 Kbps BC7: 0 Kbps
```

*A:Dut-A#*

---

**range**

**Syntax**

```
range [area-id]
```

**Context**

```
show>router>ospf
```

**Description**

This command displays ranges of addresses on an Area Border Router (ABR) for the purpose of route summarization or suppression.

**Parameters**

- **area-id** — Display the configured ranges for the specified area.

**Output**

**OSPF Range Output** — The following table describes the OSPF range output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Id</td>
<td>A 32-bit integer uniquely identifying an area. Area ID 0.0.0.0 is used for the OSPF backbone.</td>
</tr>
<tr>
<td>Address/Mask</td>
<td>The mask for the range expressed as a decimal integer mask length or in dotted decimal notation.</td>
</tr>
<tr>
<td>Advertise</td>
<td>False — The specified address/mask is not advertised outside the area.</td>
</tr>
<tr>
<td></td>
<td>True — The specified address/mask is advertised outside the area.</td>
</tr>
</tbody>
</table>

---

Page 404  
7450 ESS OS Routing Protocols Guide
Sample Output

```
A:ALA-A# show router ospf 1 range

OSPF Ranges

<table>
<thead>
<tr>
<th>Area Id</th>
<th>Address/Mask</th>
<th>Advertise</th>
<th>LSDB Type</th>
</tr>
</thead>
</table>

No. of Ranges: 0

A:ALA-A#
```

```
A:ALA-A# show router ospf range 180.0.7.9

OSPF Ranges for Area Id: 180.0.7.9

<table>
<thead>
<tr>
<th>Area Id</th>
<th>Address/Mask</th>
<th>Advertise</th>
<th>LSDB Type</th>
</tr>
</thead>
</table>

No. of Ranges: 0

A:ALA-A#
```

routes

**Syntax**
```
routes [ip-prefix[/prefix-length]] [type] [detail] [alternative] [summary]
```

**Context**
```
show>router>ospf
```

**Description**
This command information about OSPF routes.

**Parameters**
- `ip-prefix[/prefix-length]` — Displays information about the specified IP prefix and length.
- `type` — Displays information about the specified type.
  - **Values**
    - intra-area, inter-area, external-1, external-2, nssa-1, nssa-2
- `detail` — Displays detailed information about the routes.
- `alternative` — Displays the level of protection per prefix (ref. show router isis routes alternative)
- `summary` — Displays summarized information about the routes.

**Label** | **Description (Continued)**
--- | ---
LSDB Type | NSSA — This range was specified in the NSSA context, and specifies that the range applies to external routes (via type-7 LSAs) learned within the NSSA when the routes are advertised to other areas as type-5 LSAs.

**Summary** — This range was not specified in the NSSA context, the range applies to summary LSAs even if the area is an NSSA.
Sample Output

*A:Dut-A# show router ospf routes alternative detail

OSPFv2 Routing Table (detailed)

<table>
<thead>
<tr>
<th>Destination</th>
<th>Type (Dest)</th>
<th>Stat</th>
<th>NHIP</th>
<th>NHIF</th>
<th>Cost [E2]</th>
<th>Area</th>
<th>Tunnel-Information</th>
<th>PGID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.2.0/24</td>
<td>IA (NET)</td>
<td>D (F)</td>
<td>DIRECT</td>
<td>2</td>
<td>10</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.3.0/24</td>
<td>IA (NET)</td>
<td>D (F)</td>
<td>DIRECT</td>
<td>3</td>
<td>10</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.3.0/24</td>
<td>IA (NET)</td>
<td>N (R)</td>
<td>1.1.2.2</td>
<td>2</td>
<td>20</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.3.3</td>
<td></td>
<td></td>
<td>1.1.3.3</td>
<td>3</td>
<td>20</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.4.0/24</td>
<td>IA (NET)</td>
<td>N (R)</td>
<td>1.1.2.2</td>
<td>2</td>
<td>20</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.3.3(L)</td>
<td>3</td>
<td>30</td>
<td>LINK</td>
<td>0x130015</td>
<td></td>
</tr>
<tr>
<td>1.3.5.0/24</td>
<td>IA (NET)</td>
<td>N (R)</td>
<td>1.1.3.3</td>
<td>3</td>
<td>20</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.2.2(L)</td>
<td>2</td>
<td>30</td>
<td>LINK</td>
<td>0x130016</td>
<td></td>
</tr>
<tr>
<td>1.4.5.0/24</td>
<td>IA (NET)</td>
<td>N (R)</td>
<td>1.1.2.2</td>
<td>2</td>
<td>30</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.3.3</td>
<td>3</td>
<td>30</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4.6.0/24</td>
<td>IA (NET)</td>
<td>N (R)</td>
<td>1.1.3.3</td>
<td>3</td>
<td>30</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.3.3(L)</td>
<td>3</td>
<td>40</td>
<td>LINK</td>
<td>0x130015</td>
<td></td>
</tr>
<tr>
<td>1.5.6.0/24</td>
<td>IA (NET)</td>
<td>N (R)</td>
<td>1.1.3.3</td>
<td>3</td>
<td>30</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.2.2(L)</td>
<td>2</td>
<td>40</td>
<td>LINK</td>
<td>0x130016</td>
<td></td>
</tr>
<tr>
<td>10.20.1.1/32</td>
<td>IA (HOST)</td>
<td>D (F)</td>
<td>DIRECT</td>
<td>1</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.2/32</td>
<td>IA (HOST)</td>
<td>N (R)</td>
<td>1.1.2.2</td>
<td>2</td>
<td>10</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.3.3(L)</td>
<td>3</td>
<td>20</td>
<td>LINK</td>
<td>0x130015</td>
<td></td>
</tr>
<tr>
<td>10.20.1.3/32</td>
<td>IA (HOST)</td>
<td>N (R)</td>
<td>1.1.3.3</td>
<td>3</td>
<td>10</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.2.2(L)</td>
<td>2</td>
<td>20</td>
<td>LINK</td>
<td>0x130016</td>
<td></td>
</tr>
<tr>
<td>10.20.1.4/32</td>
<td>IA (HOST)</td>
<td>N (R)</td>
<td>1.1.2.2</td>
<td>2</td>
<td>20</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.3.3(L)</td>
<td>3</td>
<td>30</td>
<td>LINK</td>
<td>0x130015</td>
<td></td>
</tr>
<tr>
<td>10.20.1.5/32</td>
<td>IA (HOST)</td>
<td>N (R)</td>
<td>1.1.3.3</td>
<td>3</td>
<td>20</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.2.2(L)</td>
<td>2</td>
<td>30</td>
<td>LINK</td>
<td>0x130016</td>
<td></td>
</tr>
<tr>
<td>10.20.1.6/32</td>
<td>IA (HOST)</td>
<td>N (R)</td>
<td>1.1.3.3</td>
<td>3</td>
<td>30</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.1.2.2</td>
<td>2</td>
<td>30</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.2/0</td>
<td>IA (RTR)</td>
<td>N (N)</td>
<td>1.1.2.2</td>
<td>2</td>
<td>10</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.3/0</td>
<td>IA (RTR)</td>
<td>N (N)</td>
<td>1.1.3.3</td>
<td>3</td>
<td>10</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.4/0</td>
<td>IA (RTR)</td>
<td>N (N)</td>
<td>1.1.2.2</td>
<td>2</td>
<td>20</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.5/0</td>
<td>IA (RTR)</td>
<td>N (N)</td>
<td>1.1.3.3</td>
<td>3</td>
<td>20</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.6/0</td>
<td>IA (RTR)</td>
<td>N (N)</td>
<td>1.1.2.2</td>
<td>2</td>
<td>30</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.1.3.3  3  30  0.0.0.0
1.1.2.2  2  30  0.0.0.0

19 OSPFv2 routes found (23 paths)
Flags: L = Loop-Free Alternate nexthop

*A:Dut-A#
Show Commands

spf

Syntax  

spf [lfa]

Context  

show>router>ospf

Description  
This command displays statistics of shortest-path-first (SPF) calculations.

Parameters  

lfa — Displays Loop-Free Alternate (LFA) next-hop information.

Output  

SPF Output Fields — The following table describes SPF output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total SPF Runs</td>
<td>The total number of incremental SPF runs triggered by new or updated LSAs.</td>
</tr>
<tr>
<td>Last Full SPF run @</td>
<td>The date and time when the external OSPF Dijkstra (SPF) was last run.</td>
</tr>
<tr>
<td>Last Full SPF Time</td>
<td>The length of time, in seconds, when the last full SPF was run.</td>
</tr>
<tr>
<td>Intra SPF Time</td>
<td>The time when intra-area SPF was last run on this area.</td>
</tr>
<tr>
<td>Inter SPF Time</td>
<td>The total number of incremental SPF runs triggered by new or updated type-3 and type-4 summary LSAs.</td>
</tr>
<tr>
<td>Extern SPF Time</td>
<td>The total number of incremental SPF runs triggered by new or updated type-5 external LSAs.</td>
</tr>
<tr>
<td>RTM Updt Time</td>
<td>The time, in hundredths of seconds, used to perform a total SPF calculation.</td>
</tr>
<tr>
<td>Min/Avg/Max Full SPF Time</td>
<td>Min — The minimum time, in hundredths of seconds, used to perform a total SPF calculation. Avg — The average time, in hundredths of seconds, of all the total SPF calculations performed by this OSPF router. Max — The maximum time, in hundredths of seconds, used to perform a total SPF calculation.</td>
</tr>
<tr>
<td>Total Sum Incr SPF Runs</td>
<td>The total number of incremental SPF runs triggered by new or updated type-3 and type-4 summary LSAs.</td>
</tr>
<tr>
<td>Total Ext Incr SPF Runs</td>
<td>The total number of incremental SPF runs triggered by new or updated type-5 external LSAs.</td>
</tr>
</tbody>
</table>

Sample Output

A:Dut-A# show router ospf spf lfa
---------------------------------------------------------------
OSPF SPF Statistics
---------------------------------------------------------------
Total SPF Runs    :  6
Last Full SPF run @ : 02/20/2012 09:19:35
Last Full SPF Time : < 0.01 secs
Intra SPF Time     :  < 0.01 secs
Inter SPF Time     :  < 0.01 secs
Extern SPF Time    :  < 0.01 secs
RTM Updt Time      :  < 0.01 secs

Min/Avg/Max Full SPF Times : 0.00/0.00/0.00 secs
Min/Avg/Max RTM Updt Times : 0.00/0.00/0.00 secs

Total SPF Runs          : 109
Last Full SPF run @     : 11/07/2006 18:43:07
Last Full SPF Time      : < 0.01 secs
Intra SPF Time          : < 0.01 secs
Inter SPF Time          : < 0.01 secs
Extern SPF Time         : < 0.01 secs
RTM Updt Time           : < 0.01 secs

Min/Avg/Max Full SPF Times : 0.02/0.00/0.06 secs
Min/Avg/Max RTM Updt Times : 0.02/0.00/0.06 secs

Total Sum Incr SPF Runs : 333
Last Sum Incr SPF run @ : 11/07/2006 18:43:09
Last Sum Incr Calc Time : < 0.01 secs

Total Ext Incr SPF Runs : 0
**statistics**

**Syntax**
```
statistics
```

**Context**
```
show>router>ospf
```

**Description**
This command displays the global OSPF statistics.

**Output**
**OSPF Statistics Output Fields** — The following table describes the command output fields for OSPF statistics.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Packets</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Tx Packets</td>
<td>The total number of OSPF packets transmitted on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Rx Hellos</td>
<td>The total number of OSPF Hello packets received on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Tx Hellos</td>
<td>The total number of OSPF Hello packets transmitted on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Rx DBDs</td>
<td>The total number of OSPF database description packets received on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Tx DBDs</td>
<td>The total number of OSPF database description packets transmitted on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Rx LSRs</td>
<td>The total number of OSPF Link State Requests (LSRs) received on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Tx LSRs</td>
<td>The total number of OSPF Link State Requests (LSRs) transmitted on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Rx LSUs</td>
<td>The total number of OSPF Link State Update (LSUs) received on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Tx LSUs</td>
<td>The total number of OSPF Link State Update (LSUs) transmitted on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Rx LS Acks</td>
<td>The total number of OSPF Link State Acknowledgements (LSAs) received on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>New LSAs Recvd</td>
<td>The total number of new OSPF Link State Advertisements received on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>New LSAs Orig</td>
<td>The total number of new OSPF Link State Advertisements originated on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Ext LSAs Count</td>
<td>The total number of OSPF External Link State Advertisements.</td>
</tr>
<tr>
<td>No of Areas</td>
<td>The number of areas configured for this OSPF instance.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Total SPF Runs</td>
<td>The total number of incremental SPF runs triggered by new or updated LSAs.</td>
</tr>
<tr>
<td>Ext SPF Runs</td>
<td>The total number of incremental SPF runs triggered by new or updated type-5 external LSAs.</td>
</tr>
<tr>
<td>Retransmits</td>
<td>The total number of OSPF Retransmits transmitted on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Discards</td>
<td>The total number of OSPF packets discarded on all OSPF enabled interfaces.</td>
</tr>
<tr>
<td>Bad Networks</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces with invalid network or mask.</td>
</tr>
<tr>
<td>Bad Virt Links</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces that are destined to a virtual link that does not exist.</td>
</tr>
<tr>
<td>Bad Areas</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces with an area mismatch.</td>
</tr>
<tr>
<td>Bad Dest Addr</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces with the incorrect IP destination address.</td>
</tr>
<tr>
<td>Bad Auth Types</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces with an invalid authorization type.</td>
</tr>
<tr>
<td>Auth Failures</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces with an invalid authorization key.</td>
</tr>
<tr>
<td>Bad Neighbors</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces where the neighbor information does not match the information this router has for the neighbor.</td>
</tr>
<tr>
<td>Bad Pkt Types</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces with an invalid OSPF packet type.</td>
</tr>
<tr>
<td>Bad Lengths</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces with a total length not equal to the length given in the packet itself.</td>
</tr>
<tr>
<td>Bad Hello Int.</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces where the hello interval given in packet was not equal to that configured for the respective interface.</td>
</tr>
<tr>
<td>Bad Dead Int.</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces where the dead interval given in the packet was not equal to that configured for the respective interface.</td>
</tr>
<tr>
<td>Bad Options</td>
<td>The total number of OSPF packets received on all OSPF enabled interfaces with an option that does not match those configured for the respective interface or area.</td>
</tr>
</tbody>
</table>
Sample Output

A:ALA-A# show router ospf 1 statistics

OSPF Statistics

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Packets</td>
<td>308462 Rx Packets received.</td>
</tr>
<tr>
<td>Tx Packets</td>
<td>246800 Tx Packets transmitted.</td>
</tr>
<tr>
<td>Rx Hellos</td>
<td>173796 Rx Hellos received.</td>
</tr>
<tr>
<td>Tx Hellos</td>
<td>149062 Tx Hellos transmitted.</td>
</tr>
<tr>
<td>Rx DBDs</td>
<td>67 Rx DBDs received.</td>
</tr>
<tr>
<td>Tx DBDs</td>
<td>48 Tx DBDs transmitted.</td>
</tr>
<tr>
<td>Rx LSRs</td>
<td>21 Rx LSRs received.</td>
</tr>
<tr>
<td>Tx LSRs</td>
<td>19 Tx LSRs transmitted.</td>
</tr>
<tr>
<td>Rx LSUs</td>
<td>105672 Rx LSUs received.</td>
</tr>
<tr>
<td>Tx LSUs</td>
<td>65530 Tx LSUs transmitted.</td>
</tr>
<tr>
<td>Rx LS Acks</td>
<td>28906 Rx LS Acks received.</td>
</tr>
<tr>
<td>Tx LS Acks</td>
<td>32141 Tx LS Acks transmitted.</td>
</tr>
<tr>
<td>New LSAs Recvd</td>
<td>38113 New LSAs received.</td>
</tr>
<tr>
<td>New LSAs Orig</td>
<td>21067 New LSAs originated.</td>
</tr>
<tr>
<td>Ext LSAs Count</td>
<td>17 Ext LSAs received.</td>
</tr>
<tr>
<td>No of Areas</td>
<td>3 No of areas existed.</td>
</tr>
<tr>
<td>Total SPF Runs</td>
<td>327 Total SPF runs.</td>
</tr>
<tr>
<td>Ext SPF Runs</td>
<td>0 Ext SPF runs.</td>
</tr>
<tr>
<td>Retransmits</td>
<td>46 Retransmits.</td>
</tr>
<tr>
<td>Discards</td>
<td>0 Discards.</td>
</tr>
<tr>
<td>Bad Networks</td>
<td>0 Bad networks.</td>
</tr>
<tr>
<td>Bad Virt Links</td>
<td>0 Bad virtual links.</td>
</tr>
<tr>
<td>Bad Areas</td>
<td>0 Bad areas.</td>
</tr>
<tr>
<td>Bad Dest Addrs</td>
<td>0 Bad destinations.</td>
</tr>
<tr>
<td>Bad Auth Types</td>
<td>0 Bad authentication types.</td>
</tr>
<tr>
<td>Auth Failures</td>
<td>0 Authentication failures.</td>
</tr>
<tr>
<td>Bad Neighbors</td>
<td>0 Bad neighbors.</td>
</tr>
<tr>
<td>Bad Pkt Types</td>
<td>0 Bad packet types.</td>
</tr>
<tr>
<td>Bad Lengths</td>
<td>0 Bad lengths.</td>
</tr>
<tr>
<td>Bad Hello Int.</td>
<td>0 Bad hello interval.</td>
</tr>
<tr>
<td>Bad Options</td>
<td>0 Bad options.</td>
</tr>
<tr>
<td>Bad Versions</td>
<td>0 Bad versions.</td>
</tr>
<tr>
<td>Bad Checksums</td>
<td>0 Bad checksums.</td>
</tr>
<tr>
<td>Failed SPF Attempts</td>
<td>0 Failed SPF attempts.</td>
</tr>
<tr>
<td>CSPFF Requests</td>
<td>0 CSPFF requests.</td>
</tr>
<tr>
<td>CSPFF Request Drops</td>
<td>0 CSPFF request drops.</td>
</tr>
<tr>
<td>CSPFF Path Found</td>
<td>0 CSPFF path found.</td>
</tr>
<tr>
<td>CSPFF Path Not Found</td>
<td>0 CSPFF path not found.</td>
</tr>
</tbody>
</table>

A:ALA-A#
status

**Syntax**

`status`

**Context**

`show>router>ospf`

**Description**

Displays the general status of OSPF.

**Output**

**OSPF Status Output Fields** — The following table describes the command output fields for OSPF status.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router Id</td>
<td>A 32-bit integer uniquely identifying the router in the Autonomous System. The SR-OS system defaults to the System IP address or if not configured the 32 least significant bits of the system MAC address.</td>
</tr>
<tr>
<td>OSPF Version</td>
<td>The current version number of the OSPF protocol is 2.</td>
</tr>
<tr>
<td>OSPF Admin Status</td>
<td>Disabled — Denotes that the OSPF process is disabled on all interfaces. Enabled — Denotes that the OSPF process is active on at least one interface.</td>
</tr>
<tr>
<td>OSPF Oper Status</td>
<td>Disabled — Denotes that the OSPF process is not operational on all interfaces. Enabled — Denotes that the OSPF process is operational on at least one interface.</td>
</tr>
<tr>
<td>Preference</td>
<td>The route preference for OSPF internal routes.</td>
</tr>
<tr>
<td>External Preference</td>
<td>The route preference for OSPF external routes.</td>
</tr>
<tr>
<td>Backbone Router</td>
<td>False — This variable indicates that this router is not configured as an OSPF back bone router.</td>
</tr>
<tr>
<td></td>
<td>True — This variable indicates that this router is configured as an OSPF back bone router.</td>
</tr>
<tr>
<td>Area Border Router</td>
<td>False — This router is not an area border router.</td>
</tr>
<tr>
<td></td>
<td>True — This router is an area border router.</td>
</tr>
<tr>
<td>AS Border Router</td>
<td>False — This router is not configured as an Autonomous System border router.</td>
</tr>
<tr>
<td></td>
<td>True — This router is configured as an Autonomous System border router.</td>
</tr>
<tr>
<td>OSPF Ldp Sync Admin Status</td>
<td>Indicates whether the IGP-LDP synchronization feature is enabled or disabled on all interfaces participating in the OSPF routing protocol.</td>
</tr>
</tbody>
</table>
Sample Output

A:SetupCLI# show router ospf status
===============================================================================
OSPF Status
===============================================================================
OSPF Cfg Router Id : 255.255.255.255
OSPF Oper Router Id : 10.20.30.40
OSPF Version : 2
OSPF Admin Status : Enabled
OSPF Oper Status : Enabled
Graceful Restart : Disabled
GR Helper Mode : Disabled
Preference : 11
External Preference : 150
Backbone Router : True
Area Border Router : False
AS Border Router : True
Opaque LSA Support : True
Traffic Engineering Support : True
RFC 1583 Compatible : True
Demand Exts Support : False
In Overload State : True (Indefinitely in overload)
In External Overflow State : False
Exit Overflow Interval : 0
Last Overflow Entered : Never
Last Overflow Exit : 10/01/2011 07:34:03
External LSA Limit : -1
Reference Bandwidth : 10,000 Kbps
Init SPF Delay : 10000 msec
Sec SPF Delay : 10000 msec
Max SPF Delay : 12000 msec
Min LS Arrival Interval : 600000 msec
Init LSA Gen Delay : 100 msec
Sec LSA Gen Delay : 400 msec
Max LSA Gen Delay : 600000 msec
Last Ext SPF Run : Never
Ext LSA Cksum Sum : 0x0
OSPF Last Enabled : 10/01/2011 07:34:03
Multicast Import : False
Export Policies : test 567890123456789012345678901
: test 567890123456789012345678902
: test 567890123456789012345678903
: test 567890123456789012345678904
: test 567890123456789012345678905
Import Policies : test 567890123456789012345678901
: test 567890123456789012345678902
: test 567890123456789012345678903
: test 567890123456789012345678904
: test 567890123456789012345678905
OSPF Ldp Sync Admin Status : Disabled
LDP-over-RSVP : Enabled
RSVP-Shortcut : Enabled
Advertise-Tunnel-Link : Enabled
LFA : Enabled
Export Limit : 0
Export Limit Log Percent : 0
Total Exp Routes : 0
===============================================================================

A:SetupCLI#

A:ALA-A#  show router ospf 1 status

OSPF Status

OSPF Router Id               : 10.13.7.165
OSPF Version                 : 2
OSPF Admin Status            : Enabled
OSPF Oper Status             : Enabled
Graceful Restart             : Enabled
GR Helper Mode               : Disabled
Preference                   : 10
External Preference          : 150
Backbone Router              : True
Area Border Router           : True
AS Border Router             : True
Opaque LSA Support           : True
Traffic Engineering Support  : True
RFC 1583 Compatible          : True
TOS Routing Support          : False
Demand Exts Support          : False
In Overload State            : False
In External Overflow State   : False
Exit Overflow Interval       : 0
Last Overflow Entered        : Never
Last Overflow Exit           : Never
External LSA Limit           : -1
Reference Bandwidth          : 100,000,000 Kbps
Init SPF Delay               : 500 msec
Sec SPF Delay                : 2000 msec
Max SPF Delay                : 15000 msec
Min LS Arrival Interval      : 500 msec
Max LSA Gen Delay            : 5000 msec
Last Ext SPF Run             : Never
Ext LSA Cksum Sum            : 0x2afce
OSPF Last Enabled            : 05/23/2006 23:34:36
Export Policies              : export-static

A:ALA-A#
virtual-link

Syntax  virtual-link [detail]

Context  show>router>ospf

Description  This command displays information for OSPF virtual links.

Parameters  
- detail — Provides operational and statistical information about virtual links associated with this router.

Output  OSPF Virtual Link Output — The following table describes OSPF virtual-link output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nbr Rtr ID</td>
<td>The router ID(s) of neighboring routers.</td>
</tr>
<tr>
<td>Area Id</td>
<td>A 32-bit integer which identifies an area.</td>
</tr>
<tr>
<td>Local Interface</td>
<td>The IP address of the local egress interface used to maintain the adjacency to reach this virtual neighbor.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric value associated with the route. This value is used when importing this static route into other protocols. When the metric is configured as zero then the metric configured in OSPF, default-import-metric, applies. This value is also used to determine which static route to install in the forwarding table.</td>
</tr>
<tr>
<td>State</td>
<td>The operational state of the virtual link to the neighboring router.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Specifies whether authentication is enabled for the interface or virtual link.</td>
</tr>
<tr>
<td>Hello Intrvl</td>
<td>Specifies the length of time, in seconds, between the Hello packets that the router sends on the interface.</td>
</tr>
<tr>
<td>Rtr Dead Intrvl</td>
<td>Specifies the total number of OSPF packets received where the dead interval given in the packet was not equal to that configured on this interface since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Tot Rx Packets</td>
<td>Specifies the total number of OSPF packets received on this interface since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Rx Hellos</td>
<td>Specifies the total number of OSPF Hello packets received on this interface since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Rx DBDs</td>
<td>Specifies the total number of OSPF DataBase Description packets received on this interface since the OSPF administrative status was enabled.</td>
</tr>
<tr>
<td>Rx LSRs</td>
<td>Specifies the total number of Link State Requests (LSRs) received on this interface since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Rx LSUs</td>
<td>Specifies the total number of Link State Updates (LSUs) received on this interface since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Rx LS Ack</td>
<td>Specifies the total number of Link State Acknowledgements received on this interface since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Tot Tx Packets</td>
<td>Specifies the total number of OSPF packets transmitted on this virtual interface since it was created.</td>
</tr>
<tr>
<td>Tx Hellos</td>
<td>Specifies the total number of OSPF Hello packets transmitted on this virtual interface since it was created.</td>
</tr>
<tr>
<td>Tx DBDs</td>
<td>Specifies the total number of OSPF database description packets transmitted on this virtual interface.</td>
</tr>
<tr>
<td>Tx LSRs</td>
<td>Specifies the total number of OSPF Link State Requests (LSRs) transmitted on this virtual interface.</td>
</tr>
<tr>
<td>Tx LSUs</td>
<td>Specifies the total number of OSPF Hello packets transmitted on this interface since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Tx LS Ack</td>
<td>Specifies the total number of OSPF Link State Acknowledgements (LSA) transmitted on this virtual interface.</td>
</tr>
<tr>
<td>Retransmits</td>
<td>Specifies the total number of OSPF retransmits sent on this interface since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Discards</td>
<td>Specifies the total number of OSPF packets discarded on this interface since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Networks</td>
<td>Specifies the total number of OSPF packets received with invalid network or mask since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Versions</td>
<td>Specifies the total number of OSPF packets received with bad OSPF version numbers since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Areas</td>
<td>Specifies the total number of OSPF packets received with an area mismatch since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Dest Addrs</td>
<td>Specifies the total number of OSPF packets received with the incorrect IP destination address since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Auth Types</td>
<td>Specifies the total number of OSPF packets received with an invalid authorization type since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Auth Failures</td>
<td>Specifies the total number of OSPF packets received with an invalid authorization key since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Neighbors</td>
<td>Specifies the total number of OSPF packets received where the neighbor information does not match the information this router has for the neighbor since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Pkt Types</td>
<td>Specifies the total number of OSPF packets received with an invalid OSPF packet type since the OSPF admin status was last enabled.</td>
</tr>
</tbody>
</table>
Sample Output

A:ALA-A# show router ospf 1 virtual-link
------------------------------------------------------------------
OSPF Virtual Links
------------------------------------------------------------------
Nbr Rtr Id  Area Id        Local Interface     Metric State
------------------------------------------------------------------
180.0.0.10  0.0.0.1         180.1.7.12          300    PToP
180.0.0.10  0.0.0.2         180.2.7.12          300    PToP
------------------------------------------------------------------
No. of OSPF Virtual Links: 2
------------------------------------------------------------------
A:ALA-A#

A:ALA-A# show router ospf virtual-link detail
------------------------------------------------------------------
OSPF Virtual Links (detailed)
------------------------------------------------------------------
Neighbor Router Id : 180.0.0.10
------------------------------------------------------------------
Nbr Router Id : 180.0.0.10      Area Id : 0.0.0.1
Local Interface: 180.1.7.12     Metric : 300

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad Lengths</td>
<td>Specifies the total number of OSPF packets received on this interface with a total length not equal to the length given in the packet itself since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Hello Int.</td>
<td>Specifies the total number of OSPF packets received where the hello interval given in packet was not equal to that configured on this interface since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Dead Int.</td>
<td>Specifies the total number of OSPF packets received where the dead interval given in the packet was not equal to that configured on this interface since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Options</td>
<td>Specifies the total number of OSPF packets received with an option that does not match those configured for this interface or area since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Retrans Intrvl</td>
<td>Specifies the length of time, in seconds, that OSPF waits before retransmitting an unacknowledged link state advertisement (LSA) to an OSPF neighbor.</td>
</tr>
<tr>
<td>Transit Delay</td>
<td>Specifies the time, in seconds, that it takes to transmit a link state advertisement (LSA) on the interface or virtual link.</td>
</tr>
<tr>
<td>Last Event</td>
<td>Specifies the date and time when an event was last associated with this OSPF interface.</td>
</tr>
</tbody>
</table>
State : Point To Point  Admin State : Up
Hello Intrvl : 10 sec  Rtr Dead Intrvl : Up
Tot Rx Packets : 43751  Tot Tx Packets : 43751
Rx Hellos : 24851  Tx Hellos : 24851
Rx DBDs : 3  Tx DBDs : 2
Rx LSRs : 1  Tx LSRs : 1
Rx LSUs : 18071  Tx LSUs : 18071
Rx LS Acks : 147  Tx LS Acks : 334
Retransmits : 0  Discards : 0
Bad Networks : 0  Bad Versions : 0
Bad Areas : 0  Bad Dest Addr : 0
Bad Auth Types : 0  Auth Failures : 0
Bad Neighbors : 0  Bad Pkt Types : 0
Bad Lengths : 0  Bad Hello Int. : 0
Bad Dead Int. : 0  Bad Options : 0
Retrans Intrvl : 5 sec  Transit Delay : 1 sec
Last Event : 11/07/2006 17:11:56  Authentication : None

Neighbor Router Id : 180.0.0.10

Nbr Router Id : 180.0.0.10  Area Id : 0.0.0.2
Local Interface: 180.2.7.12  Metric : 300
State : Point To Point  Admin State : Up
Hello Intrvl : 10 sec  Rtr Dead Intrvl : Up
Tot Rx Packets : 43751  Tot Tx Packets : 43751
Rx Hellos : 24851  Tx Hellos : 24851
Rx DBDs : 3  Tx DBDs : 2
Rx LSRs : 1  Tx LSRs : 1
Rx LSUs : 18071  Tx LSUs : 18071
Rx LS Acks : 147  Tx LS Acks : 334
Retransmits : 0  Discards : 0
Bad Networks : 0  Bad Versions : 0
Bad Areas : 0  Bad Dest Addr : 0
Bad Auth Types : 0  Auth Failures : 0
Bad Neighbors : 0  Bad Pkt Types : 0
Bad Lengths : 0  Bad Hello Int. : 0
Bad Dead Int. : 0  Bad Options : 0
Retrans Intrvl : 5 sec  Transit Delay : 1 sec
Last Event : 11/07/2006 17:12:00  Authentication : MD5

A:ALA-A#
virtual-neighbor

**Syntax**
```
virtual-neighbor [remote router-id] [detail]
```

**Context**
```
show>router>ospf
```

**Description**
This command displays virtual neighbor information.

**Parameters**
- **remote router-id** — Displays the specified router ID. This reduces the amount of output displayed.
- **detail** — Produces detailed information on the virtual neighbor. This option produces a large amount of data. It is recommended to use `detail` only when requesting information for a specific neighbor.

**Output**

**OSPF Virtual Neighbor Output** — The following table describes OSPF virtual neighbor output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nbr IP Addr</td>
<td>The IP address this neighbor is using in its IP source address. Note that, on addressless links, this will not be 0.0.0.0, but the address of another of the neighbor's interfaces.</td>
</tr>
<tr>
<td>Nbr Rtr ID</td>
<td>Specifies the router ID(s) of neighboring routers.</td>
</tr>
<tr>
<td>Transit Area</td>
<td>Specifies the transit area ID that links the backbone area with the area that has no physical connection with the backbone.</td>
</tr>
<tr>
<td>Retrans Q Length</td>
<td>The current length of the retransmission queue.</td>
</tr>
<tr>
<td>No. of Neighbors</td>
<td>Specifies the total number of OSPF neighbors adjacent on this interface, in a state of INIT or greater, since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Nbr State</td>
<td>Specifies the operational state of the virtual link to the neighboring router.</td>
</tr>
<tr>
<td>Options</td>
<td>Specifies the total number of OSPF packets received with an option that does not match those configured for this virtual interface or transit area since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Events</td>
<td>Specifies the total number of events that have occurred since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Last Event Time</td>
<td>Specifies the date and time when an event was last associated with this OSPF interface.</td>
</tr>
<tr>
<td>Up Time</td>
<td>Specifies the uninterrupted time, in hundredths of seconds, the adjacency to this neighbor has been up.</td>
</tr>
<tr>
<td>Time Before Dead</td>
<td>Specifies the amount of time, in seconds, until the dead router interval expires.</td>
</tr>
<tr>
<td>Bad Nbr States</td>
<td>Specifies the total number of OSPF packets received where the neighbor information does not match the information this router has for the neighbor since the OSPF admin status was last enabled.</td>
</tr>
</tbody>
</table>
### Sample Output

**A:ALA-A# show router ospf 1 virtual-neighbor**

<table>
<thead>
<tr>
<th>Nbr IP Addr</th>
<th>Nbr Rtr Id</th>
<th>Nbr State</th>
<th>Transit Area</th>
<th>RetxQ Len</th>
<th>Dead Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>180.1.6.10</td>
<td>180.0.0.10</td>
<td>Full</td>
<td>0.0.0.1</td>
<td>0</td>
<td>58</td>
</tr>
<tr>
<td>180.2.9.10</td>
<td>180.0.0.10</td>
<td>Full</td>
<td>0.0.0.2</td>
<td>0</td>
<td>52</td>
</tr>
</tbody>
</table>

No. of Neighbors: 2

**A:ALA-A#**

**A:ALA-A# show router ospf virtual-neighbor detail**

<table>
<thead>
<tr>
<th>Neighbor IP Addr</th>
<th>Neighbor Rtr Id</th>
<th>Neighbor State</th>
<th>Transit Area</th>
<th>Retrans Q Length</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>180.1.6.10</td>
<td>180.0.0.10</td>
<td>Full</td>
<td>0.0.0.1</td>
<td>0</td>
<td>-E--</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSA Inst fails</td>
<td>Specifies the total number of times an LSA could not be installed into the LSDB due to a resource allocation issue since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad Seq Nums</td>
<td>Specifies the total number of times when a database description packet was received with a sequence number mismatch since the OSPF admin status was last enabled.</td>
</tr>
<tr>
<td>Bad MTUs</td>
<td>Specifies the total number of times when the MTU in a received database description packet was larger than the MTU of the receiving interface since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Bad Packets</td>
<td>Specifies the total number of times when an LS update was received with an illegal LS type or an option mismatch since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>LSA not in LSDB</td>
<td>Specifies the total number of times when an LS request was received for an LSA not installed in the LSDB of this router since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Option Mismatches</td>
<td>Specifies the total number of times when a LS update was received with an option mismatch since the OSPF admin status was enabled.</td>
</tr>
<tr>
<td>Nbr Duplicates</td>
<td>Specifies the total number of times when a duplicate database description packet was received during the Exchange state since the OSPF admin status was enabled.</td>
</tr>
</tbody>
</table>
Show Commands

Events : 4  Last Event Time : 11/07/2006 17:11:56
Up Time : 2d 17:47:17  Time Before Dead : 57 sec
Bad Nbr States : 1  LSA Inst fails : 0
Bad Seq Nums : 0  Bad MTUs : 0
Bad Packets : 0  LSA not in LSDB : 0
Option Mismatches : 0  Nbr Duplicates : 0

-----------------------------------------------------------------------------
Virtual Neighbor Router Id : 180.0.0.10
-----------------------------------------------------------------------------
Neighbor IP Addr : 180.2.9.10  Neighbor Rtr Id : 180.0.0.10
Neighbor State : Full  Transit Area : 0.0.0.2
Retrans Q Length : 0  Options : -E--
Up Time : 2d 17:47:14  Time Before Dead : 59 sec
Bad Nbr States : 1  LSA Inst fails : 0
Bad Seq Nums : 0  Bad MTUs : 0
Bad Packets : 0  LSA not in LSDB : 0
Option Mismatches : 0  Nbr Duplicates : 0

-----------------------------------------------------------------------------
A:ALA-A#
Clear Commands

ospf

Syntax  
ospf [ ospf-instance ]

Context  
clear>router

Description  
This command clears and resets OSPF protocol entities.

Parameters  
ospf-instance — Clears the configured specified VR-ID.

Values  
1 — 4294967295

database

Syntax  
database [ purge ]

Context  
clear>router>ospf

Description  
This command clears all LSAs received from other nodes.
Sets all adjacencies better then two way to one way.
Refreshes all self originated LSAs

Parameters  
purge — The purge parameter also clears all self-originated LSAs and re-originates all self-originated LSAs

export

Syntax  
export

Context  
clear>router>ospf

Description  
Re-evaluates all effective export policies

neighbor

Syntax  
neighbor [ ip-int-name | ip-address ]

Context  
clear>router>ospf

Description  
Marks the neighbor as dead and re-initiates the affected adjacencies.

Parameters  

ip-int-name — Clear all neighbors for the interface specified by this interface name.

ip-address — Clear all neighbors for the interface specified by this IP-address
Clear Commands

statistics

Syntax statistics

Context clear>router>ospf

Description Clears all neighbor, router, interface, SPF and global statistics of this OSPF instance.
**OSPF Debug Commands**

**ospf**

**Syntax**

ospf [ospf-instance]

**Context**
debug>router

**Description**
Indicates the OSPF instance for debugging purposes.

**Parameters**

- **ospf-instance** — The OSPF instance.
  - **Values**
    - 1 — 31

**area**

**Syntax**

area [area-id]

no area

**Context**
debug>router>ospf

**Description**
This command enables debugging for an OSPF area.

**Parameters**

- **area-id** — Specify the OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

**area-range**

**Syntax**

area-range [ip-address]

no area-range

**Context**
debug>router>ospf

**Description**
This command enables debugging for an OSPF area range.

**Parameters**

- **ip-address** — Specify the IP address for the range used by the ABR to advertise the area into another area.

**cspf**

**Syntax**

cspf [ip-address]

no cspf

**Context**
debug>router>ospf

**Description**
This command enables debugging for an OSPF constraint-based shortest path first (CSPF).
Parameters  

*ip-address* — Specify the IP address for the range used for CSPF.

**graceful-restart**

**Syntax**  

```
[no] graceful-restart
```

**Context**  

debug>router>ospf

**Description**  

This command enables debugging for OSPF graceful-restart.

**interface**

**Syntax**  

```
interface [ip-int-name | ip-address]
no interface
```

**Context**  

debug>router>ospf

**Description**  

This command enables debugging for an OSPF interface.

**Parameters**  

*ip-int-name* — Specify the IP interface name. An interface name cannot be in the form of an IP address.

Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

*ip-address* — Specify the interface’s IP address.
leak

Syntax  
leak [ip-address]
no leak

Context  debug>router>ospf

Description  This command enables debugging for OSPF leaks.

Parameters  ip-address — Specify the IP address to debug OSPF leaks.

lsdb

Syntax  
lsdb [type] [ls-id] [adv-rtr-id] [area area-id]
no lsdb

Context  debug>router>ospf

Description  This command enables debugging for an OSPF link-state database (LSDB).

Parameters  type — Specifies the OSPF link-state database (LSDB) type.

Values  router, network, summary, asbr, extern, nssa, area-opaque, as-opaque, link-opaque

ls-id — Specifies an LSA type specific field containing either a router ID or an IP address. It identifies the piece of the routing domain being described by the advertisement.

adv-rtr-id — Specifies the router identifier of the router advertising the LSA.

area-id — Specifies a 32-bit integer uniquely identifying an area.

misc

Syntax  
[no] misc

Context  debug>router>ospf

Description  This command enables debugging for miscellaneous OSPF events.

neighbor

Syntax  
neighbor [ip-int-name | ip-address]
no neighbor

Context  debug>router>ospf

Description  This command enables debugging for an OSPF neighbor.

Parameters  ip-int-name — Specifies the neighbor interface name.
ip-address — Specifies neighbor information for the neighbor identified by the specified router ID.

 NSSA Range

Syntax  nssa-range [ip-address]

no nssa-range

Context  debug>router>ospf

Description  This command enables debugging for an NSSA range.

Parameters  ip-address — Specifies the IP address range to debug.

Packet

Syntax  packet [packet-type] [ip-address]

no packet

Context  debug>router>ospf

Description  This command enables debugging for OSPF packets.

Parameters  packet-type — Specifies the OSPF packet type to debug.

Values  hello, dbdescr, lsrequest, lsupdate, lsack

ip-address — Specifies the IP address to debug.

Values  ipv4-address: a.b.c.d

RTM

Syntax  rtm [ip-address]

no rtm

Context  debug>router>ospf

Description  This command enables debugging for OSPF RTM.

Parameters  ip-address — Specifies the IP address to debug.

Values  ipv4-address: a.b.c.d
spf

Syntax
spf [type] [dest-addr]
no spf

Context
debug>router>ospf

Description
This command enables debugging for OSPF SPF. Information regarding overall SPF start and stop times will be shown. To see detailed information regarding the SPF calculation of a given route, the route must be specified as an optional argument.

Parameters

type — Specifies the area to debug

Values
intra-area, inter-area, external

dest-addr — Specifies the destination IP address to debug.

virtual-neighbor

Syntax
virtual-neighbor [ip-address]
no virtual-neighbor

Context
debug>router>ospf

Description
This command enables debugging for an OSPF virtual neighbor.

Parameters
ip-address — Specifies the IP address of the virtual neighbor.
In This Chapter

This chapter provides information to configure Intermediate System to Intermediate System (IS-IS).

Topics in this chapter include:

- Configuring IS-IS on page 432
  - Routing on page 433
    - IS-IS Frequently Used Terms on page 435
    - ISO Network Addressing on page 436
    - IS-IS Unnumbered Interfaces on page 438
    - ISO Network Addressing on page 436
    - IS-IS PDU Configuration on page 439
    - IS-IS Operations on page 439
    - IS-IS Route Summarization on page 440
    - IS-IS Administrative Tags on page 441
- IS-IS Configuration Process Overview on page 443
- Configuration Notes on page 444
Intermediate-system-to-intermediate-system (IS-IS) is a link-state interior gateway protocol (IGP) which uses the Shortest Path First (SPF) algorithm to determine routes. Routing decisions are made using the link-state information. IS-IS evaluates topology changes and, if necessary, performs SPF recalculations.

Entities within IS-IS include networks, intermediate systems, and end systems. In IS-IS, a network is an autonomous system (AS), or routing domain, with end systems and intermediate systems. A router is an intermediate system. End systems are network devices which send and receive protocol data units (PDUs), the OSI term for packets. Intermediate systems send, receive, and forward PDUs.

End system and intermediate system protocols allow routers and nodes to identify each other. IS-IS sends out link-state updates periodically throughout the network, so each router can maintain current network topology information.

IS-IS supports large ASs by using a two-level hierarchy. A large AS can be administratively divided into smaller, more manageable areas. A system logically belongs to one area. Level 1 routing is performed within an area. Level 2 routing is performed between areas. The routers can be configured as Level 1, Level 2, or both Level 1/2.

Figure 14 displays an example of an IS-IS routing domain.
Routing

OSI IS-IS routing uses two-level hierarchical routing. A routing domain can be partitioned into areas. Level 1 routers know the topology in their area, including all routers and end systems in their area but do not know the identity of routers or destinations outside of their area. Level 1 routers forward traffic with destinations outside of their area to a Level 2 router in their area.

Level 2 routers know the Level 2 topology, and know which addresses are reachable by each Level 2 router. Level 2 routers do not need to know the topology within any Level 1 area, except to the extent that a Level 2 router can also be a Level 1 router within a single area. By default, only Level 2 routers can exchange PDUs or routing information directly with external routers located outside the routing domain.

In IS-IS, there are two types of routers:

- Level 1 intermediate systems — Routing is performed based on the area ID portion of the ISO address called the *network entity title* (NET). Level 1 systems route within an area. They recognize, based on the destination address, whether the destination is within the area. If so, they route toward the destination. If not, they route to the nearest Level 2 router.
- Level 2 intermediate systems — Routing is performed based on the area address. They route toward other areas, disregarding other area’s internal structure. A Level 2 intermediate system can also be configured as a Level 1 intermediate system in the same area.

The Level 1 router’s area address portion is manually configured (see ISO Network Addressing on page 436). A Level 1 router will not become a neighbor with a node that does not have a common area address. However, if a Level 1 router has area addresses A, B, and C, and a neighbor has area addresses B and D, then the Level 1 router will accept the other node as a neighbor, as address B is common to both routers. Level 2 adjacencies are formed with other Level 2 nodes whose area addresses do not overlap. If the area addresses do not overlap, the link is considered by both routers to be Level 2 only and only Level 2 LSPDUs flow on the link.

Within an area, Level 1 routers exchange LSPs which identify the IP addresses reachable by each router. Specifically, zero or more IP address, subnet mask, and metric combinations can be included in each LSP. Each Level 1 router is manually configured with the IP address, subnet mask, and metric combinations, which are reachable on each interface. A Level 1 router routes as follows:

- If a specified destination address matches an IP address, subnet mask, or metric reachable within the area, the PDU is routed via Level 1 routing.
- If a specified destination address does not match any IP address, subnet mask, or metric combinations listed as reachable within the area, the PDU is routed towards the nearest Level 2 router.
Level 2 routers include in their LSPs, a complete list of IP address, subnet mask, and metrics specifying all the IP addresses which reachable in their area. This information can be obtained from a combination of the Level 1 LSPs (by Level 1 routers in the same area). Level 2 routers can also report external reachability information, corresponding to addresses reachable by routers in other routing domains or autonomous systems.
IS-IS Frequently Used Terms

- Area — An area is a routing sub-domain which maintains detailed routing information about its own internal composition, and also maintains routing information which allows it to reach other routing sub-domains. Areas correspond to the Level 1 sub-domain.
- End system — End systems send NPDUs to other systems and receive NPDUs from other systems, but do not relay NPDUs. This International Standard does not specify any additional end system functions beyond those supplied by ISO 8473 and ISO 9542.
- Neighbor — A neighbor is an adjacent system reachable by traversing a single sub-network by a PDU.
- Adjacency — An adjacency is a portion of the local routing information which pertains to the reachability of a single neighboring end or intermediate system over a single circuit. Adjacencies are used as input to the decision process to form paths through the routing domain. A separate adjacency is created for each neighbor on a circuit and for each level of routing (Level 1 and Level 2) on a broadcast circuit.
- Circuit — The subset of the local routing information base pertinent to a single local Subnetwork Point of Attachments (SNPAs).
- Link — The communication path between two neighbors. A link is up when communication is possible between the two SNPAs.
- Designated IS — The intermediate system on a LAN which is designated to perform additional duties. In particular, the designated IS generates link-state PDUs on behalf of the LAN, treating the LAN as a pseudonode.
- Pseudonode — Where a broadcast sub-network has $n$ connected intermediate systems, the broadcast sub-network itself is considered to be a pseudonode. The pseudonode has links to each of the $n$ intermediate systems and each of the ISs has a single link to the pseudonode (rather than $n-1$ links to each of the other intermediate systems). Link-state PDUs are generated on behalf of the pseudonode by the designated IS.
- Broadcast sub-network — A multi-access subnetwork that supports the capability of addressing a group of attached systems with a single PDU.
- General topology sub-network — A topology that is modeled as a set of point-to-point links, each of which connects two systems. There are several generic types of general topology subnetworks, multipoint links, permanent point-to-point links, dynamic and static point-to-point links.
- Routing sub-domain — A routing sub-domain consists of a set of intermediate systems and end systems located within the same routing domain.
- Level 2 sub-domain — Level 2 sub-domain is the set of all Level 2 intermediate systems in a routing domain.
ISO Network Addressing

IS-IS uses ISO network addresses. Each address identifies a point of connection to the network, such as a router interface, and is called a Network Service Access Point (NSAP).

An end system can have multiple NSAP addresses, in which case the addresses differ only by the last byte (called the n-selector). Each NSAP represents a service that is available at that node. In addition to having multiple services, a single node can belong to multiple areas.

Each network entity has a special network address called a Network Entity Title (NET). Structurally, an NET is identical to an NSAP address but has an n-selector of 00. Most end systems have one NET. Intermediate systems can have up to three area IDs (area addresses).

NSAP addresses are divided into three parts. Only the area ID portion is configurable.

- Area ID — A variable length field between 1 and 13 bytes long. This includes the Authority and Format Identifier (AFI) as the most significant byte and the area ID.
- System ID — A six-byte system identification. This value is not configurable. The system ID is derived from the system or router ID.
- Selector ID — A one-byte selector identification that must contain zeros when configuring a NET. This value is not configurable. The selector ID is always 00.

Of the total 20 bytes comprising the NET, only the first 13 bytes, the area ID portion, can be manually configured. As few as one byte can be entered or, at most, 13 bytes. If less than 13 bytes are entered, the rest is padded with zeros.

Routers with common area addresses form Level 1 adjacencies. Routers with no common NET addresses form Level 2 adjacencies, if they are capable (Figure 15).
Figure 15: Using Area Addresses to Form Adjacencies
IS-IS Unnumbered Interfaces

IS-IS support for unnumbered point-to-point links include Ethernet interfaces both on access SAPs and network SAPs. This is part of a phased approach to support unnumbered links. Some features that use IS-IS, such as MPLS, do not yet support unnumbered links.
IS-IS PDU Configuration

The following PDUs are used by IS-IS to exchange protocol information:

- IS-IS hello PDU — Routers with IS-IS enabled send hello PDUs to IS-IS-enabled interfaces to discover neighbors and establish adjacencies.
- Link-state PDUs — Contain information about the state of adjacencies to neighboring IS-IS systems. LSPs are flooded periodically throughout an area.
- Complete sequence number PDUs — In order for all routers to maintain the same information, CSNPs inform other routers that some LSPs can be outdated or missing from their database. CSNPs contain a complete list of all LSPs in the current IS-IS database.
- Partial sequence number PDUs (PSNPs) — PSNPs are used to request missing LSPs and acknowledge that an LSP was received.

IS-IS Operations

The routers perform IS-IS routing as follows:

- Hello PDUs are sent to the IS-IS-enabled interfaces to discover neighbors and establish adjacencies.
- IS-IS neighbor relationships are formed if the hello PDUs contain information that meets the criteria for forming an adjacency.
- ESSs can build a link-state PDU based upon their local interfaces that are configured for IS-IS and prefixes learned from other adjacent routers.
- ESSs flood LSPs to the adjacent neighbors except the neighbor from which they received the same LSP. The link-state database is constructed from these LSPs.
- A Shortest Path Tree (SPT) is calculated by each IS, and from this SPT the routing table is built.
IS-IS Route Summarization

IS-IS IPv4 route summarization allows users to create aggregate IPv4 addresses that include multiple groups of IPv4 addresses for a given IS-IS level. IPv4 Routes redistributed from other routing protocols also can be summarized. It is similar to the OSPF area-range command. IS-IS IPv4 route summarization helps to reduce the size of the LSDB and the IPv4 routing table, and it also helps to reduce the chance of route flapping.

IPv4 route summarization supports:

- Level 1, Level 1-2, and Level 2
- Route summarization for the IPv4 routes redistributed from other protocols
- Metric used to advertise the summary address will be the smallest metric of all the more specific IPv4 routes.
IS-IS Administrative Tags

IS-IS admin tags enable a network administrator to configure route tags to tag IS-IS route prefixes. These tags can subsequently be used to control Intermediate System-to-Intermediate System (IS-IS) route redistribution or route leaking.

The IS-IS support for route tags allows the tagging of IP addresses of an interface and use the tag to apply administrative policy with a route map. A network administrator can also tag a summary route and then use a route policy to match the tag and set one or more attributes for the route.

Using these administrative policies allow the operator to control how a router handles the routes it receives from and sends to its IS-IS neighboring routers. Administrative policies are also used to govern the installation of routes in the routing table.

Route tags allow:

- Policies to redistribute routes received from other protocols in the routing table to IS-IS.
- Policies to redistribute routes between levels in an IS-IS routing hierarchy.
- Policies to summarize routes redistributed into IS-IS or within IS-IS by creating aggregate (summary) addresses.

Setting Route Tags

IS-IS route tags are configurable in the following ways:

- Setting a route tag for an IS-IS interface.
- Setting a route tag on an IS-IS passive interface.
- Setting a route tag for a route redistributed from another protocol to IS-IS.
- Setting a route tag for a route redistributed from one IS-IS level to another IS-IS level.
- Setting a route tag for an IS-IS default route.
- Setting a route tag for an IS-IS summary address.
Using Route Tags

Although an operator on this or another (neighboring) IS-IS router has configured setting of the IS-IS administrative tags it will not have any effect unless policies are configure to instruct how to process the given tag value.

Policies can process tags where ISIS is either the origin, destination or both origin and destination protocol.

```
config>router>policy-options>policy-statement>entry>from
    config>router>policy-options>policy-statement>entry>action tag tag-value
    config>router>policy-options>policy-statement# default-action tag tag-value
```
IS-IS Configuration Process Overview

Figure 16 displays the process to provision basic IS-IS parameters.

START

ENABLE IS-IS

CONFIGURE GLOBAL PARAMETERS

MODIFY LEVEL-CAPABILITY (OPTIONAL)

CONFIGURE INTERFACE PARAMETERS

ENSABLE

SPECIFY AREA ADDRESSES

Figure 16: IS-IS Configuration and Implementation Flow
Configuration Notes

This section describes IS-IS configuration caveats.

General

- IS-IS must be enabled on each participating router.
- There are no default network entity titles.
- There are no default interfaces.
- By default, the routers are assigned a Level 1/Level 2 level capability.
Configuring IS-IS with CLI

This section provides information to configure intermediate-system-to-intermediate-system (IS-IS) using the command line interface.

Topics in this section include:

- **IS-IS Configuration Overview on page 446**
  - Router Levels on page 446
  - Area Address Attributes on page 446
  - Interface Level Capability on page 447
  - Route Leaking on page 448
- **Basic IS-IS Configuration on page 449**
- **Common Configuration Tasks on page 451**
  - Enabling IS-IS on page 452
  - Modifying Router-Level Parameters on page 452
  - Configuring ISO Area Addresses on page 454
  - Configuring Global IS-IS Parameters on page 455
  - Configuring Interface Parameters on page 456
- **IS-IS Configuration Management Tasks on page 461**
  - Disabling IS-IS on page 461
  - Modifying Global IS-IS Parameters on page 462
  - Modifying IS-IS Interface Parameters on page 463
  - Example: Configuring a Level 1 Area on page 458
  - Example: Modifying a Router's Level Capability on page 460
  - Configuring Leaking on page 465
  - Redistributing External IS-IS Routers on page 468
  - Specifying MAC Addresses for All IS-IS Routers on page 469
Router Levels

The router’s level capability can be configured globally and on a per-interface basis. The interface-level parameters specify the interface’s routing level. The neighbor capability and parameters define the adjacencies that are established.

IS-IS is not enabled by default. When IS-IS is enabled, the global default level capability is Level 1/2 which enables the router to operate as either a Level 1 and/or a Level 2 router with the associated databases. The router runs separate shortest path first (SPF) calculations for the Level 1 area routing and for the Level 2 multi-area routing to create the IS-IS routing table.

The level value can be modified on both or either of the global and interface levels to be only Level 1-capable, only Level 2-capable or Level 1 and Level 2-capable.

If the default value is not modified on any routers in the area, then the routers try to form both Level 1 and Level 2 adjacencies on all IS-IS interfaces. If the default values are modified to Level 1 or Level 2, then the number of adjacencies formed are limited to that level only.

Area Address Attributes

The area-id command specifies the area address portion of the NET which is used to define the IS-IS area to which the router will belong. At least one area-id command should be configured on each router participating in IS-IS. A maximum of three area-id commands can be configured per router.

The area address identifies a point of connection to the network, such as a router interface, and is called a network service access point (NSAP). The routers in an area manage routing tables about destinations within the area. The Network Entity Title (NET) value is used to identify the IS-IS area to which the router belongs.

NSAP addresses are divided into three parts. Only the Area ID portion is configurable.

1. Area ID — A variable length field between 1 and 13 bytes long. This includes the Authority and Format Identifier (AFI) as the most significant byte and the area ID.
2. System ID — A six-byte system identification. This value is not configurable. The system ID is derived from the system or router ID.
3. Selector ID — A one-byte selector identification that must contain zeros when configuring a NET. This value is not configurable. The selector ID is always 00.
The following example displays ISO addresses in IS-IS address format:

MAC address 00:a5:c7:6b:c4:90 49.0011.00a5.c76b.c490.00
IP address: 218.112.14.5 49.0011.2181.1201.4005.00

### Interface Level Capability

The level capability value configured on the interface level is compared to the level capability value configured on the global level to determine the type of adjacencies that can be established. The default level capability for routers and interfaces is Level 1/2.

Table 12 displays configuration combinations and the potential adjacencies that can be formed.

**Table 12: Potential Adjacency Capabilities**

<table>
<thead>
<tr>
<th>Global Level</th>
<th>Interface Level</th>
<th>Potential Adjacency</th>
</tr>
</thead>
<tbody>
<tr>
<td>L 1/2</td>
<td>L 1/2</td>
<td>Level 1 and/or Level 2</td>
</tr>
<tr>
<td>L 1/2</td>
<td>L 1</td>
<td>Level 1 only</td>
</tr>
<tr>
<td>L 1/2</td>
<td>L 2</td>
<td>Level 2 only</td>
</tr>
<tr>
<td>L 2</td>
<td>L 1/2</td>
<td>Level 2 only</td>
</tr>
<tr>
<td>L 2</td>
<td>L 2</td>
<td>Level 2 only</td>
</tr>
<tr>
<td>L 2</td>
<td>L 1</td>
<td>none</td>
</tr>
<tr>
<td>L 1</td>
<td>L 1/2</td>
<td>Level 1 only</td>
</tr>
<tr>
<td>L 1</td>
<td>L 2</td>
<td>none</td>
</tr>
<tr>
<td>L 1</td>
<td>L 1</td>
<td>Level 1 only</td>
</tr>
</tbody>
</table>
Route Leaking

Alcatel-Lucent’s implementation of IS-IS route leaking is performed in compliance with RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*. As previously stated, IS-IS is a routing domain (an autonomous system running IS-IS) which can be divided into Level 1 areas with a Level 2-connected subset (backbone) of the topology that interconnects all of the Level 1 areas. Within each Level 1 area, the routers exchange link state information. Level 2 routers also exchange Level 2 link state information to compute routes between areas.

Routers in a Level 1 area typically only exchange information within the Level 1 area. For IP destinations not found in the prefixes in the Level 1 database, the Level 1 router forwards PDUs to the nearest router that is in both Level 1/Level 2 with the *attached bit* set in its Level 1 link-state PDU.

There are many reasons to implement domain-wide prefix distribution. The goal of domain-wide prefix distribution is to increase the granularity of the routing information within the domain. The routing mechanisms specified in RFC 1195 are appropriate in many situations and account for excellent scalability properties. However, in certain circumstances, the amount of scalability can be adjusted which can distribute more specific information than described by RFC 1195.

Distributing more prefix information can improve the quality of the resulting routes. A well known property of default routing is that loss of information can occur. This loss of information affects the computation of a route based upon less information which can result in sub-optimal routes.
Basic IS-IS Configuration

For IS-IS to operate on the routers, IS-IS must be explicitly enabled, and at least one area address and interface must be configured. If IS-IS is enabled but no area address or interface is defined, the protocol is enabled but no routes are exchanged. When at least one area address and interface are configured, then adjacencies can be formed and routes exchanged.

To configure IS-IS, perform the following tasks:

- Enable IS-IS.
- If necessary, modify the level capability on the global level (default is level-1/2).
- Define area address(es)
- Configure IS-IS interfaces.

The following output displays IS-IS default values.

```
A:Dut-A>config>router>isis$ info detail
----------------------------------------------
level-capability level-1/2
no graceful-restart
area-id 01
no authentication-key
no authentication-type
authentication-check
csnp-authentication
lsp-lifetime 1200
no export
hello-authentication
psnp-authentication
traffic-engineering
no reference-bandwidth
no disable-ldp-sync
ipv4-routing
spf-wait 10 1000 1000
no strict-adjacency-check
lsp-wait 5 0 1
level 1
  no authentication-key
  no authentication-type
  csnp-authentication
  external-preference 160
  hello-authentication
  preference 15
  psnp-authentication
  no wide-metrics-only
exit
level 2
  no authentication-key
  no authentication-type
  csnp-authentication
  external-preference 165
  hello-authentication
```
Basic IS-IS Configuration

preference 18
psnp-authentication
no wide-metrics-only
exit
no shutdown

----------------------------------------------
A:Dut-A>config>router>isis$
Common Configuration Tasks

To implement IS-IS in your network, you must enable IS-IS on each participating router.

To assign different level capabilities to the routers and organize your network into areas, modify the level capability defaults on end systems from Level 1/2 to Level 1. Routers communicating to other areas can retain the Level 1/2 default.

On each router, at least one area ID also called the area address should be configured as well as at least one IS-IS interface.

• Enable IS-IS.
• Configure global IS-IS parameters.
  → Configure area address(es).
• Configure IS-IS interface-specific parameters.
Configuring IS-IS Components

Use the CLI syntax displayed below for:

- Enabling IS-IS on page 452
- Modifying Router-Level Parameters on page 452
- Configuring ISO Area Addresses on page 454
- Configuring Global IS-IS Parameters on page 455
- Configuring Interface Parameters on page 456
- Example: Configuring a Level 1 Area on page 458
- Example: Modifying a Router’s Level Capability on page 460

---

Enabling IS-IS

IS-IS must be enabled in order for the protocol to be active.

NOTE: Careful planning is essential to implement commands that can affect the behavior of global and interface levels.

To configure IS-IS on a router, enter the following command:

**CLI Syntax:** `isis`

**Example:** `config-router# isis`

---

Modifying Router-Level Parameters

When IS-IS is enabled, the default level-capability is Level 1/2. This means that the router operates with both Level 1 and Level 2 routing capabilities. To change the default value in order for the router to operate as a Level 1 router or a Level 2 router, you must explicitly modify the level value.

If the level is modified, the protocol shuts down and restarts. Doing this can affect adjacencies and routes.

The level-capability value can be configured on the global level and also on the interface level. The level-capability value determines which level values can be assigned on the router level or on an interface-basis.
In order for the router to operate as a Level 1 only router or as a Level 2 only router, you must explicitly specify the `level-number` value.

- Select `level-1` to route only within an area.
- Select `level-2` to route to destinations outside an area, toward other eligible Level 2 routers.

To configure the router level, enter the following commands:

**CLI Syntax:**
```
config>router# isis
   level-capability {level-1|level-2|level-1/2}
   level {1|2}
```

**Example:**
```
config>router# isis
config>router>isis# level-capability 1/2
config>router>isis# level 2
```

The following example displays the configuration:

```
A:ALA-A>config>router>isis# info
#------------------------------------------
echo "ISIS"
#------------------------------------------
   level-capability level-1/2
   level 2
#------------------------------------------
A:ALA-A>config>router>isis#
```
Configuring ISO Area Addresses

Use the following CLI syntax to configure an area ID also called an address. A maximum of 3 area-id can be configured.

**CLI Syntax:**
```
config>router# isis
    area-id area-address
```

The following example configures the router’s area ID:

**Example:**
```
config>router>isis#
    config>router>isis# area-id 49.0180.0001
    config>router>isis# area-id 49.0180.0002
    config>router>isis# area-id 49.0180.0003
```

The following example displays the area ID configuration:

```
A:ALA-A>config>router>isis# info
 ----------------------------------------------
 area-id 49.0180.0001
 area-id 49.0180.0002
 area-id 49.0180.0003
 ----------------------------------------------
A:ALA-A>config>router>isis#
```


**Configuring Global IS-IS Parameters**

Commands and parameters configured on the global level are inherited to the interface levels. Parameters specified in the interface and interface-level configurations take precedence over global configurations.

The following example displays global-level IS-IS configuration command usage:

**Example:**
```
config>router# isis
config>router>isis#
config>router>isis# level-capability level-2
config>router>isis# authentication-check
config>router>isis# authentication-type password
config>router>isis# authentication-key test
config>router>isis# overload timeout 90
config>router>isis# traffic-engineering
```

The following example displays the modified global-level configuration.

```
A:ALA-A>config>router>isis# info
----------------------------------------------
   level-capability level-2
   area-id 49.0180.0001
   area-id 49.0180.0002
   area-id 49.0180.0003
   authentication-key "H5KBAWzAAQU" hash
   authentication-type password
   overload timeout 90
   traffic-engineering
----------------------------------------------
A:ALA-A>config>router>isis#
```
Configuring Interface Parameters

There are no interfaces associated with IS-IS by default. An interface belongs to all areas configured on a router. Interfaces cannot belong to separate areas. There are no default interfaces applied to the router’s IS-IS instance. You must configure at least one IS-IS interface in order for IS-IS to work.

To enable IS-IS on an interface, first configure an IP interface in the `config>router>` interface context. Then, apply the interface in the `config>router>isis>interface` context.

You can configure both the Level 1 parameters and the Level 2 parameters on an interface. The `level-capability` value determines which level values are used.

NOTE: For point-to-point interfaces, only the values configured under Level 1 are used regardless of the operational level of the interface.

The following example displays the modified interface parameters:

**Example:**
```
config>router# isis
config>router>isis# level 1
config>router>isis>level# wide-metrics-only
config>router>isis>level# exit
config>router>isis# level 2
config>router>isis>level# wide-metrics-only
config>router>isis>level# exit
config>router>isis# interface ALA-1-2
config>router>isis>if# level-capability level-2
config>router>isis>if# mesh-group 85
config>router>isis>if# exit
config>router>isis# interface ALA-1-3
config>router>isis>if# level-capability level-1
config>router>isis>if# interface-type point-to-point
config>router>isis>if# mesh-group 101
config>router>isis>if# exit
config>router>isis# interface ALA-1-5
config>router>isis>if# level-capability level-1
config>router>isis>if# interface-type point-to-point
config>router>isis>if# mesh-group 85
config>router>isis>if# exit
config>router>isis# interface to-103
config>router>isis>if# level-capability level-1/2
>router>isis>if# mesh-group 101
config>router>isis>if# exit
config>router>isis#
```
The following example displays the global and interface-level configurations.

```
A:ALA-A>config>router>isis# info
----------------------------------------------
level-capability level-2
area-id 49.0180.0001
area-id 49.0180.0002
area-id 49.0180.0003
authentication-key "H5KBAWrAAQU" hash
authentication-type password
traffic-engineering
level 1
   wide-metrics-only
exit
level 2
   wide-metrics-only
exit
interface "system"
exi
interface "ALA-1-2"
   level-capability level-2
   mesh-group 85
exit
interface "ALA-1-3"
   level-capability level-1
   interface-type point-to-point
   mesh-group 101
exit
interface "ALA-1-5"
   level-capability level-1
   interface-type point-to-point
   mesh-group 85
exit
interface "to-103"
   mesh-group 101
exit
----------------------------------------------
A:ALA-A>config>router>isis#
```
Example: Configuring a Level 1 Area

NOTE: Interfaces are configured in the `config>router>interface` context.

![Diagram showing Level 1 Area configuration]

The following example displays the command usage to configure a Level 1 area.

```
A:ALA-A>config>router# isis
A:ALA-A>config>router>isis# area-id 47.0001
A:ALA-A>config>router>isis# level-capability level-1
A:ALA-A>config>router>isis# interface system
A:ALA-A>config>router>isis>if# exit
A:ALA-A>config>router>isis# interface A-B
A:ALA-A>config>router>isis>if# exit
A:ALA-A>config>router>isis# interface A-C
A:ALA-A>config>router>isis>if# exit
A:ALA-A>config>router>isis#

A:ALA-B>config>router# isis
A:ALA-B>config>router>isis# area-id 47.0001
A:ALA-B>config>router>isis# level-capability level-1
A:ALA-B>config>router>isis# interface system
A:ALA-B>config>router>isis>if# exit
A:ALA-B>config>router>isis# interface B-A
A:ALA-B>config>router>isis>if# exit
A:ALA-B>config>router>isis# interface B-C
A:ALA-B>config>router>isis>if# exit
A:ALA-B>config>router>isis#

A:ALA-C>config>router# isis
A:ALA-C>config>router>isis# area-id 47.0001
A:ALA-C>config>router>isis# level-capability level-1
A:ALA-C>config>router>isis# interface system
```
A:ALA-C>config>router>isis>if# exit
A:ALA-C>config>router>isis# interface "C-A"
A:ALA-C>config>router>isis>if# exit
A:ALA-C>config>router>isis# interface "C-B"
A:ALA-C>config>router>isis>if# exit

A:ALA-A>config>router>isis# info
----------------------------------------------
  level-capability level-1
  area-id 49.0180.0001
  interface "system"
  exit
  interface "A-B"
  exit
  interface "A-C"
  exit
----------------------------------------------
A:ALA-A>config>router>isis#

A:ALA-B>config>router>isis# info
----------------------------------------------
  level-capability level-1
  area-id 49.0180.0001
  interface "system"
  exit
  interface "B-A"
  exit
  interface "B-C"
  exit
----------------------------------------------
A:ALA-B>config>router>isis#

A:ALA-C>config>router>isis# info
#------------------------------------------
echo "ISIS"
----------------------------------------------
  level-capability level-1
  area-id 49.0180.0001
  interface "system"
  exit
  interface "C-A"
  exit
  interface "C-B"
  exit
----------------------------------------------
A:ALA-C>config>router>isis#
Example: Modifying a Router’s Level Capability

In the previous example, ALA-A, ALA-B, and ALA-C are configured as Level 1 systems. Level 1 systems communicate with other Level 1 systems in the same area. In this example, ALA-A is modified to set the level capability to Level 1/2. Now, the Level 1 systems in the area with NET 47.0001 forward PDUs to ALA-A for destinations that are not in the local area.

Figure 18: Configuring a Level 1/2 Area

The following example displays the command usage to configure a Level 1/2 system.

A:ALA-A>config>router# isis
A:ALA-A>config>router>isis# level-capability level-1/2
IS-IS Configuration Management Tasks

This section discusses the following IS-IS configuration management tasks:

- Disabling IS-IS on page 461
- Removing IS-IS on page 461
- Modifying Global IS-IS Parameters on page 462
- Modifying IS-IS Interface Parameters on page 463
  → Example: Configuring a Level 1 Area on page 458
  → Example: Modifying a Router’s Level Capability on page 460
- Configuring Leaking on page 465
- Redistributing External IS-IS Routers on page 468
- Specifying MAC Addresses for All IS-IS Routers on page 469

Disabling IS-IS

The `shutdown` command disables the IS-IS protocol instance on the router. The configuration settings are not changed, reset, or removed.

To disable IS-IS on a router, enter the following commands:

**CLI Syntax:** `config>router# isis
shutdown`

Removing IS-IS

The `no isis` command deletes the IS-IS protocol instance. The IS-IS configuration reverts to the default settings.

To remove the IS-IS configuration enter the following commands:

**CLI Syntax:** `config>router#
no isis`
Modifying Global IS-IS Parameters

You can modify, disable, or remove global IS-IS parameters without shutting down entities. Changes take effect immediately. Modifying the level capability on the global level causes the IS-IS protocol to restart.

The following example displays command usage to modify various parameters:

Example:  config>router>isis# overload timeout 500
          config>router>isis# level-capability level-1/2
          config>router>isis# no authentication-check
          config>router>isis# authentication-key raiderslost

The following example displays the global modifications

```
A:ALA-A>config>router>isis# info
----------------------------------------------
  area-id 49.0180.0001
  area-id 49.0180.0002
  area-id 49.0180.0003
  authentication-key "//oZrvtvFPn06S42lRIJsE" hash
  authentication-type password
  no authentication-check
  overload timeout 500 on-boot
  level 1
      wide-metrics-only
  exit
  level 2
      wide-metrics-only
  exit
  interface "system"
  exit
  interface "ALA-1-2"
      level-capability level-2
      mesh-group 85
  exit
  interface "ALA-1-3"
      level-capability level-1
      interface-type point-to-point
      mesh-group 101
  exit
  interface "ALA-1-5"
      level-capability level-1
      interface-type point-to-point
      mesh-group 85
  exit
  interface "to-103"
      mesh-group 101
  exit
  interface "A-B"
  exit
  interface "A-C"
  exit
----------------------------------------------
A:ALA-A>config>router>isis#
```
Modifying IS-IS Interface Parameters

You can modify, disable, or remove interface-level IS-IS parameters without shutting down entities. Changes take effect immediately. Modifying the level capability on the interface causes the IS-IS protocol on the interface to restart.

To remove an interface, issue the `no interface ip-int-name` command.
To disable an interface, issue the `shutdown` command in the interface context.

The following example displays interface IS-IS modification command usage:

Example: `config>router# isis`
```plaintext
config>router>isis# interface ALA-1-3
config>router>isis>if# mesh-group 85
config>router>isis>if# passive
config>router>isis>if# lsp-pacing-interval 5000
config>router>isis>if# exit
config>router>isis# interface to-103
config>router>isis>if# hello-authentication-type message-digest
config>router>isis>if# hello-authentication-key 49ersrule
config>router>isis>if# exit
```

The following example displays the modified interface parameters.

A:ALA-A>config>router>isis# info
```
----------------------------------------------
area-id 49.0180.0001
area-id 49.0180.0002
area-id 49.0180.0003
authentication-key "/oZrvtvFPn06S42lRIJsE" hash
authentication-type password
no authentication-check
overload timeout 500 on-boot
level 1
   wide-metrics-only
exit
level 2
   wide-metrics-only
exit
interface "system"
exit
interface "ALA-1-2"
   level-capability level-2
   mesh-group 85
exit
interface "ALA-1-3"
   level-capability level-1
   interface-type point-to-point
   lsp-pacing-interval 5000
   mesh-group 85
   passive
exit
interface "ALA-1-5"
```
level-capability level-1
interface-type point-to-point
mesh-group 85
exit
interface "to-103"
  hello-authentication-key "DvR31264KQ6vXMTvbAIImE" hash
  hello-authentication-type message-digest
  mesh-group 101
exit
interface "A-B"
exit

----------------------------------------------
A:ALA-A>config>router>isis#
Configuring Leaking

IS-IS allows a two-level hierarchy to route PDUs. Level 1 areas can be interconnected by a contiguous Level 2 backbone.

The Level 1 link-state database contains information only about that area. The Level 2 link-state database contains information about the Level 2 system and each of the Level 1 systems in the area. A Level 1/2 router contains information about both Level 1 and Level 2 databases. A Level 1/2 router advertises information about its Level 1 area toward the other Level 1/2 or Level 2 (only) routers.

Packets with destinations outside the Level 1 area are forwarded toward the closest Level 1/2 router which, in turn, forwards the packets to the destination area.

Sometimes, the shortest path to an outside destination is not through the closest Level 1/2 router, or, the only Level 1/2 system to forward packets out of an area is not operational. Route leaking provides a mechanism to leak Level 2 information to Level 1 systems to provide routing information regarding inter-area routes. Then, a Level 1 router has more options to forward packets.

Configure a route policy to leak routers from Level 2 into Level 1 areas in the config>router>policy-options>policy-statement context.

The following example shows the command usage to configure prefix list and policy statement parameters in the config>router context.

```
cfg>router>policy-options# prefix-list loops
  ..>policy-options>prefix-list# prefix 10.1.1.0/24 longer
  ..>policy-options>prefix-list# exit
  ..>policy-options# policy-statement leak
  ..>policy-options>policy-statement# entry 10
  ..>policy-options>policy-statement>entry# from
  ..>policy-options>policy-statement>entry>from# prefix-list loops
  ..>policy-options>policy-statement>entry>from# level 2
  ..>policy-options>policy-statement>entry>from# exit
  ..>policy-options>policy-statement>entry# to
  ..>policy-options>policy-statement>entry>to# level 1
  ..>policy-options>policy-statement>entry>to# exit
  ..>policy-options>policy-statement>entry# action accept
  ..>policy-options>policy-statement>entry>action# exit
  ..>policy-options>policy-statement# exit
  ..>policy-options# commit
  ..>policy-options#
```
Next, apply the policy to leak routes from Level 2 info Level 1 systems on ALA-A.

```
config>router#isis
config>router>isis# export leak
```

```
A:ALA-A>config>router>isis# info
----------------------------------------------
area-id 49.0180.0001
area-id 49.0180.0002
area-id 49.0180.0003
authentication-key "/oZrvtvFFn06S42lRIJsE" hash
authentication-type password
no authentication-check
export "leak"
... 
----------------------------------------------
A:ALA-A>config>router>isis#
```
After the policy is applied, create a policy to redistribute external IS-IS routes from Level 1 systems into the Level 2 backbone (see Redistributing External IS-IS Routers on page 468). In the config>router context, configure the following policy statement parameters:

```
config>router>policy-options# begin
..>policy-options# policy-statement "isis-ext"
..>policy-options>policy-statement# entry 10
..>policy-options>policy-statement>entry$ from
..>policy-options>policy-statement>entry#from$ external
..>policy-options>policy-statement>entry# exit
..>policy-options>policy-statement>entry# to
..>policy-options>policy-statement>entry>to$ level 2
..>policy-options>policy-statement>entry>to# exit
..>policy-options>policy-statement>entry# action accept
..>policy-options>policy-statement>entry>action# exit
..>policy-options>policy-statement>entry# exit
..>policy-options>policy-statement# exit
..>policy-options# commit
```

```
A:ALA-A>config>router>policy-options# info
--------------------------------------------
prefix-list "loops"
 prefix 10.1.1.0/24 longer
 exit
 policy-statement "leak"
 entry 10
 from
 prefix-list "loop"
 level 2
 exit
 to
 level 1
 exit
 action accept
 exit
 exit
 exit
 policy-statement "isis-ext"
 entry 10
 from
 external
 exit
 to
 level 2
 exit
 action accept
 exit
 exit
--------------------------------------------
A:ALA-A>config>router>policy-options# info
```
Redistributing External IS-IS Routers

IS-IS does not redistribute Level 1 external routes into Level 2 by default. You must explicitly apply the policy to redistribute external IS-IS routes. Policies are created in the `config>router>policy-options` context. Refer to the Route Policy section of this manual for more information.

The following example displays the policy statement configuration.

```plaintext
config>router>policy-options# info
----------------------------------------------
 prefix-list "loops"
 prefix 10.1.1.0/24 longer
exit
policy-statement "leak"
 entry 10
 from
 prefix-list "loop"
 level 2
exit
to
 level 1
exit
action accept
exit
exit
exit
policy-statement "isis-ext"
 entry 10
 from
 external
exit
to
 level 2
exit
action accept
exit
exit
exit
exit
----------------------------------------------
config>router>policy-options#
```

Redistributing External IS-IS Routers

IS-IS does not redistribute Level 1 external routes into Level 2 by default. You must explicitly apply the policy to redistribute external IS-IS routes. Policies are created in the `config>router>policy-options` context. Refer to the Route Policy section of this manual for more information.

The following example displays the policy statement configuration.

```plaintext
config>router>policy-options# info
----------------------------------------------
 prefix-list "loops"
 prefix 10.1.1.0/24 longer
exit
policy-statement "leak"
 entry 10
 from
 prefix-list "loop"
 level 2
exit
to
 level 1
exit
action accept
exit
exit
exit
policy-statement "isis-ext"
 entry 10
 from
 external
exit
to
 level 2
exit
action accept
exit
exit
exit
----------------------------------------------
config>router>policy-options#
```
Specifying MAC Addresses for All IS-IS Routers

Specify the MAC address to use for all L1 or L2 IS-IS routers. The following example shows how to specify all L1 routers:

Example: all-l1isis 01-80-C2-00-00-14

You can also specify the MAC address for all L2 IS-IS routers by using the all-l2isis command.
IS-IS Command Reference

Command Hierarchies

Configuration Commands

- Global Commands on page 471
- Interface Commands on page 472
- Show Commands on page 473
- Clear Commands on page 474
- Debug Commands on page 474

```
config
  -- router
    -- [no] isis [instance-id]
        -- [no] advertise-passive-only
        -- [no] advertise-tunnel-links
        -- all-l1isis ieee-address
        -- no all-l1isis
        -- all-l2isis ieee-address
        -- no all-l2isis
        -- [no] area-id area-address
        -- [no] authentication-check
        -- authentication-key [authentication-key | hash-key] [hash | hash2]
        -- [no] authentication-key
        -- authentication-type {password | message-digest}
        -- [no] authentication-type
        -- [no] csnp-authentication
        -- default-route-tag tag
        -- no default-route-tag
        -- [no] disable-idp-sync
        -- export policy-name [.. policy-name]
        -- no export
        -- export-limit number [log percentage]
        -- no export-limit
        -- [no] graceful-restart
        -- [no] helper-disable
        -- [no] hello-authentication
        -- [no] ipv4-routing
        -- [no] ldp-over-rsvp
        -- level {1 | 2}
          -- authentication-key [authentication-key | hash-key] [hash | hash2]
          -- [no] authentication-key
          -- authentication-type {password | message-digest}
          -- [no] authentication-type
          -- [no] csnp-authentication
```
— default-metric ipv4 metric
— no default-metric
— default-ipv6-unicast-metric ipv6 metric
— no default-ipv6-unicast-metric
— external-preference external-preference
— no external-preference
— [no] hello-authentication
— [no] loopfree-alternate-exclude
— preference preference
— no preference
— [no] psnp-authentication
— [no] wide-metrics-only
—  level-capability {level-1 | level-2 | level-1/2}
— [no] loopfree-alternate
— lsp-lifetime seconds
— no lsp-lifetime
— lsp-mtu-size size
— no lsp-mtu-size
— [no] lsp-wait lsp-wait [lsp-initial-wait [lsp-second-wait]]
— [no] multi-topology
— [no] multicast-import
— overload [timeout seconds]
— no overload
— overload-on-boot [timeout seconds]
— no overload-on-boot
— [no] psnp-authentication
— reference-bandwidth reference-bandwidth
— no reference-bandwidth
— [no] rsvp-shortcut
— no shutdown
— [no] spf-wait spf-wait [spf-initial-wait [spf-second-wait]]
— [no] suppress-default
— summary-address {ip-prefix/mask | ip-prefix [netmask]} level [tag tag]
— no summary-address {ip-prefix/mask | ip-prefix [netmask]}
— [no] traffic-engineering
— [no] unicast-import-disable
— [no] interface ip-int-name
—  [no] bfd-enable {ipv4}
—  csnp-interval seconds
—  no csnp-interval
—  hello-authentication-key [authentication-key | hash-key][hash | hash2]
—  no hello-authentication-key
—  hello-authentication-type {password | message-digest}
—  no hello-authentication-type
—  interface-type {broadcast | point-to-point}
—  no interface-type
—  [no] metric
—  level {1 | 2}
—   hello-authentication-key [authentication-key | hash-key] [hash | hash2]
—   no hello-authentication-key
—   hello-authentication-type {password | message-digest}
—   no hello-authentication-type
—   hello-interval seconds
— no hello-interval
— hello-multiplier multiplier
— no hello-multiplier
— metric metric
— no metric
— [no] passive
— priority number
— no priority
— level-capability {level-1 | level-2 | level-1/2}
— lsp-pacing-interval milli-seconds
— no lsp-pacing-interval
— [no] loopfree-alternate-exclude
— [no] loopfree-alternate
— mesh-group {value | blocked}
— no mesh-group
— [no] passive
— retransmit-interval seconds
— no retransmit-interval
— [no] shutdown
— tag tag
— no tag

Show Commands

show
  — router
    — isis
      — adjacency [ip-address | ip-int-name | nbr-system-id] [detail]
      — database [system-id | lsp-id] [detail] [level level]
      — hostname
      — interface [ip-int-name | ip-address] [detail]
      — lfa-coverage
      — neighbor
      — routes [ipv4-unicast | mt mt-id-number | alternative | ip-prefix[/prefix-length]]
      — spf [detail] [lfa]
      — spf-log [detail]
      — statistics
      — status
      — summary-address [ip-address [/mask]]
      — topology [ipv4-unicast | mt mt-id-number] [detail]
Clear Commands

```
clear
    — router
    — isis [isis-instance]
      — adjacency [system-id]
      — database [system-id]
      — export
      — spf-log
      — statistics
```

Debug Commands

```
debuge
    — router
    — isis
      — [no] adjacency [ip-int-name | ip-address | nbr-system-id]
      — [no] espf
      — [no] graceful-restart
      — interface [ip-int-name | ip-address]
      — no interface
      — leak [ip-address]
      — no leak
      — [no] lsdb [level-number] [system-id | lsp-id]
      — [no] misc
      — packet [packet-type] [ip-int-name | ip-address] [detail]
      — rtm [ip-address]
      — no rtm
      — [no] spf [level-number] [system-id]
```
IS-IS Configuration Commands

Generic Commands

**isis**

Syntax  
isis [instance-id]  
no isis [instance-id]

Context  
config>router

Description  
This command creates the context to configure the Intermediate-System-to-Intermediate-System (IS-IS) protocol instance.

The IS-IS protocol instance is enabled with the `no shutdown` command in the `config>router>isis` context. Alternatively, the IS-IS protocol instance is disabled with the `shutdown` command in the `config>router>isis` context.

The `no` form of the command deletes the IS-IS protocol instance. Deleting the protocol instance removes all configuration parameters for this IS-IS instance.

Parameters  
`instance-id` — Specifies the instance ID for an IS-IS instance.

Values  
1–31

Default  
0

**shutdown**

Syntax  
[no] shutdown

Context  
config>router>isis
config>router>isis>interface ip-int-name
config>router>isis>if>level level-number

Description  
This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The `no` form of this command administratively enables an entity.

Special Cases  
**IS-IS Global** — In the `config>router>isis` context, the `shutdown` command disables the IS-IS protocol instance. By default, the protocol is enabled, `no shutdown`.

**IS-IS Interface** — In the `config>router>isis>interface` context, the command disables the IS-IS interface. By default, the IS-IS interface is enabled, `no shutdown`. 
IS-IS Interface and Level — In the `config>router>isis>interface ip-int-name>level` context, the command disables the IS-IS interface for the level. By default, the IS-IS interface at the level is enabled, `no shutdown`.

Default `no shutdown` — IS-IS entity is administratively enabled.
IS-IS Commands

tag

Syntax   tag tag
         no tag

Context  config>router>isis>interface

Description  This command configures a route tag to the specified IP address of an interface.

Parameters  tag — [1..4294967295]

all-l1isis

Syntax   all-l1isis ieee-address
         no all-l1isis

Context  config>router>isis

Description  This command enables you to specify the MAC address to use for all L1 IS-IS routers. The MAC address should be a multicast address. You should shut/no shut the IS-IS instance to make the change operational.

Default   all-l1isis 01-80-C2-00-01-00

Parameters  ieee-address — Specifies the destination MAC address for all L1 IS-IS neighbors on the link for this ISIS instance.

all-l2isis

Syntax   all-l2isis ieee-address
         no all-l2isis

Context  config>router>isis

Description  This command enables you to specify the MAC address to use for all L2 IS-IS routers. The MAC address should be a multicast address. You should shut/no shut the IS-IS instance to make the change operational.

Default   all-l2isis 01-80-C2-00-02-11

Parameters  ieee-address — Specifies the destination MAC address for all L2 ISIS neighbors on the link for this ISIS instance.
authentication-check

Syntax      [no] authentication-check
Context     config>router>isis
Description This command sets an authentication check to reject PDUs that do not match the type or key requirements.
The default behavior when authentication is configured is to reject all IS-IS protocol PDUs that have a mismatch in either the authentication type or authentication key.
When no authentication-check is configured, authentication PDUs are generated and IS-IS PDUs are authenticated on receipt. However, mismatches cause an event to be generated and will not be rejected.
The no form of this command allows authentication mismatches to be accepted and generate a log event.
Default    authentication-check — Rejects authentication mismatches.

authentication-key

Syntax      authentication-key [authentication-key | hash-key] [hash | hash2]
no authentication-key
Context     config>router>isis
            config>router>isis>level level-number
Description This command sets the authentication key used to verify PDUs sent by neighboring routers on the interface.
Neighboring routers use passwords to authenticate PDUs sent from an interface. For authentication to work, both the authentication key and the authentication type on a segment must match. The authentication-type statement must also be included.
To configure authentication on the global level, configure this command in the config>router>isis context. When this parameter is configured on the global level, all PDUs are authenticated including the hello PDU.
To override the global setting for a specific level, configure the authentication-key command in the config>router>isis>level context. When configured within the specific level, hello PDUs are not authenticated.
The no form of the command removes the authentication key.
Default    no authentication-key — No authentication key is configured.
Parameters  authentication-key — The authentication key. The key can be any combination of ASCII characters up to 255 characters in length (un-encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ “).
hash-key — The hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ “).
This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.
hash — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.
hash2 — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.

authentication-type

Syntax: authentication-type {password | message-digest}
no authentication

Context: config>router>isis
config>router>isis>level level-number

Description: This command enables either simple password or message digest authentication or must go in either the global IS-IS or IS-IS level context.

Both the authentication key and the authentication type on a segment must match. The authentication-key statement must also be included.

Configure the authentication type on the global level in the config>router>isis context.

Configure or override the global setting by configuring the authentication type in the config>router>isis>level context.

The no form of the command disables authentication.

Default: no authentication-type — No authentication type is configured and authentication is disabled.

Parameters:
password — Specifies that simple password (plain text) authentication is required.
message-digest — Specifies that MD5 authentication in accordance with RFC2104 is required.

bfd-enable

Syntax: [no] bfd-enable {ipv4}

Context: config>router>isis>interface

Description: This command enables the use of bi-directional forwarding (BFD) to control IPv4 adjacencies. By enabling BFD on an IPv4 or IPv6 protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set by the BFD command under the IP interface. This command must be given separately to enable/disable BFD for both IPv4 and IPv6.

The no form of this command removes BFD from the associated adjacency.

Default: no bfd-enable ipv4
default-route-tag

Syntax  
default-route-tag tag
        no default-route-tag

Context  
config>router>isis

Description  
This command configures the route tag for default route.

Parameters  
tag — tag — Assigns a default tag

Values  
Accepts decimal or hex formats:
        ISIS: [0x0..0xFFFFFFFF]H
        Values  
        1 — 4294967295

csnp-authentication

Syntax  
[no] csnp-authentication

Context  
config>router>isis
        config>router>isis>level level-number

Description  
This command enables authentication of individual ISIS packets of complete sequence number PDUs (CSNP) type.
The no form of the command suppresses authentication of CSNP packets.

csnp-interval

Syntax  
csnp-interval seconds
        no csnp-interval

Context  
config>router>isis>interface ip-int-name

Description  
This command configures the time interval, in seconds, to send complete sequence number (CSN) PDUs from the interface. IS-IS must send CSN PDUs periodically.
The no form of the command reverts to the default value.

Default  
csnp-interval 10 — CSN PDUs are sent every 10 seconds for LAN interfaces.
csnp-interval 5 — CSN PDUs are sent every 5 seconds for point-to-point interfaces.

Parameters  
seconds — The time interval, in seconds between successive CSN PDUs sent from this interface expressed as a decimal integer.

Values  
1 — 65535
default-metric

Syntax    default-metric  ipv4 metric
          no default-metric

Context    config>router>isis>level

Description   This command specifies the configurable default metric used for all IS-IS interfaces on this level. This value is not used if a metric is configured for an interface.

Default    10

  ipv4 metric — Specifies the default metric for IPv4 unicast.

    Values     1 — 16777215

default-ipv6-unicast-metric

Syntax    default-ipv6-unicast-metric  ipv6 metric
          no default-ipv6-unicast-metric

Context    config>router>isis>level

Description   This command specifies the default metric for IPv6 unicast.

Default    no default-ipv6-unicast-metric

Parameters    ipv6-metric — Specifies the default metric for IPv6 unicast.

    Values     1 — 16777215

disable-ldp-sync

Syntax    [no] disable-ldp-sync

Context    config>router>isis

Description   This command disables the IGP-LDP synchronization feature on all interfaces participating in the OSPF or IS-IS routing protocol. When this command is executed, IGP immediately advertises the actual value of the link cost for all interfaces which have the IGP-LDP synchronization enabled if the currently advertised cost is different. It will then disable IGP-LDP synchronization for all interfaces. This command does not delete the interface configuration. The no form of this command has to be entered to re-enable IGP-LDP synchronization for this routing protocol.

The no form of this command restores the default settings and re-enables IGP-LDP synchronization on all interfaces participating in the OSPF or IS-IS routing protocol and for which the ldp-sync-timer is configured.

Default    no disable-ldp-sync
export

Syntax   [no] export policy-name [policy-name...up to 5 max]
Context  config>router>isis
Description This command configures export routing policies that determine the routes exported from the routing table to IS-IS.
If no export policy is defined, non IS-IS routes are not exported from the routing table manager to IS-IS.
If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered overrides the previous command. A maximum of five policy names can be specified.
If an aggregate command is also configured in the config>router context, then the aggregation is applied before the export policy is applied.
Routing policies are created in the config>router>policy-options context.
The no form of the command removes the specified policy-name or all policies from the configuration if no policy-name is specified.
Default   no export — No export policy name is specified.
Parameters policy-name — The export policy name. Up to five policy-name arguments can be specified.

export-limit

Syntax   export-limit number [log percentage]
no export-limit
Context  config>router>isis
Description This command configures the maximum number of routes (prefixes) that can be exported into IS-IS from the route table.
The no form of the command removes the parameters from the configuration.
Default   no export-limit, the export limit for routes or prefixes is disabled.
Parameters number — Specifies the maximum number of routes (prefixes) that can be exported into RIP from the route table.
Values 1 — 4294967295
log percentage — Specifies the percentage of the export-limit, at which a warning log message and SNMP notification would be sent.
Values 1 — 100
external-preference

**Syntax**

```
external-preference preference
no external-preference
```

**Context**

```
config>router>isis>level level-number
```

**Description**

This command configures the external route preference for the IS-IS level.

The `external-preference` command configures the preference level of either IS-IS level 1 or IS-IS level 2 external routes. By default, the preferences are as listed in the table below.

A route can be learned by the router by different protocols, in which case, the costs are not comparable. When this occurs, the preference decides the route to use.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is dependent on the default preference table. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision of the route to use is determined by the configuration of the `ecmp` in the `config>router` context.

**Default**

Default preferences are listed in the following table:

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Preference</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct attached</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Static-route</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF internal routes</td>
<td>10</td>
<td>No</td>
</tr>
<tr>
<td>IS-IS Level 1 internal</td>
<td>15</td>
<td>Yes*</td>
</tr>
<tr>
<td>IS-IS Level 2 internal</td>
<td>18</td>
<td>Yes*</td>
</tr>
<tr>
<td>OSPF external</td>
<td>150</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS Level 1 external</td>
<td>160</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS Level 2 external</td>
<td>165</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Internal preferences are changed using the `preference` command in the `config>router>isis>level level-number` context

**Parameters**

`preference` — The preference for external routes at this level as expressed.

**Values**

1 — 255
graceful-restart

Syntax  [no] graceful-restart
Context  config>router>isis
Description  This command enables graceful-restart helper support for ISIS. The router will act as a helper to neighbors who are graceful-restart-capable and are restarting.

When the control plane of a graceful-restart-capable router fails, the neighboring routers (graceful-restart helpers) temporarily preserve adjacency information so packets continue to be forwarded through the failed graceful-restart router using the last known routes. If the control plane of the graceful-restart router comes back up within the timer limits, then the routing protocols re-converge to minimize service interruption.

The no form of the command disables graceful restart and removes all graceful restart configurations in the ISIS instance.

Default  disabled

helper-disable

Syntax  [no] helper-disable
Context  config>router>isis>graceful-restart
Description  This command disables the helper support for graceful restart.

When graceful-restart is enabled, the router can be a helper (meaning that the router is helping a neighbor to restart) or be a restarting router or both. The router supports only helper mode. Thisfacilitates the graceful restart of neighbors but will not act as a restarting router (meaning that the router will not help the neighbors to restart).

The no helper-disable command enables helper support and is the default when graceful-restart is enabled.

Default  disabled

hello-authentication

Syntax  [no] hello-authentication
Context  config>router>isis
           config>router>isis>level level-number
Description  This command enables authentication of individual ISIS packets of HELLO type.

The no form of the command suppresses authentication of HELLO packets.
loopfree-alternate-exclude

Syntax  
[no] loopfree-alternate

Context  
configure>router>isis>level
       configure>router>isis>interface

Description  
This command instructs IGP to not include a specific interface or all interfaces participating in a specific IS-IS level or OSPF area in the SPF LFA computation. This provides a way of reducing the LFA SPF calculation where it is not needed.

When an interface is excluded from the LFA SPF in IS-IS, it is excluded in both level 1 and level 2. When it is excluded from the LFA SPF in OSPF, it is excluded in all areas. However, the above OSPF command can only be executed under the area in which the specified interface is primary and once enabled, the interface is excluded in that area and in all other areas where the interface is secondary. If the user attempts to apply it to an area where the interface is secondary, the command will fail.

The no form of this command re-instates the default value for this command.

Default  
no loopfree-alternate-exclude

loopfree-alternate

Syntax  
[no] loopfree-alternate

Context  
config>router>isis

Description  
This command enables Loop-Free Alternate (LFA) computation by SPF under the IS-IS routing protocol level or under the OSPF routing protocol instance level.

When this command is enabled, it instructs the IGP SPF to attempt to pre-compute both a primary next-hop and an LFA next-hop for every learned prefix. When found, the LFA next-hop is populated into the routing table along with the primary next-hop for the prefix.

The no form of this command disables the LFA computation by IGP SPF.

Default  
no loopfree-alternate

hello-authentication-key

Syntax  
hello-authentication-key [authentication-key | hash-key] [hash | hash2]
no hello-authentication-key

Context  
config>router>isis>interface ip-int-name
config>router>isis>if>level level-number

Description  
This command configures the authentication key (password) for hello PDUs. Neighboring routers use the password to verify the authenticity of hello PDUs sent from this interface. Both the hello authentication key and the hello authentication type on a segment must match. The hello-authentication-type must be specified.
To configure the hello authentication key in the interface context use the `hello-authentication-key` in the `config>router>isis>interface` context.

To configure or override the hello authentication key for a specific level, configure the `hello-authentication-key` in the `config>router>isis>interface>level` context.

If both IS-IS and hello-authentication are configured, hello messages are validated using hello authentication. If only IS-IS authentication is configured, it will be used to authenticate all IS-IS (including hello) protocol PDUs.

When the hello authentication key is configured in the `config>router>isis>interface` context, it applies to all levels configured for the interface.

The `no` form of the command removes the authentication-key from the configuration.

**Default**

`no hello-authentication-key` — No hello authentication key is configured.

**Parameters**

- `authentication-key` — The hello authentication key (password). The key can be any combination of ASCII characters up to 254 characters in length (un-encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

- `hash-key` — The hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (" ").

  This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

- `hash` — Specifies the key is entered in an encrypted form. If the `hash` parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the `hash` parameter specified.

- `hash2` — Specifies the key is entered in a more complex encrypted form. If the `hash2` parameter is not used, the less encrypted `hash` form is assumed.

### hello-authentication-type

**Syntax**

```
hello-authentication-type {password | message-digest}
no hello-authentication-type
```

**Context**

- `config>router>isis>interface ip-int-name`
- `config>router>isis>if>level level-number`

**Description**

This command enables hello authentication at either the interface or level context. Both the hello authentication key and the hello authentication type on a segment must match. The hello `authentication-key` statement must also be included.

To configure the hello authentication type at the interface context, use `hello-authentication-type` in the `config>router>isis>interface` context.

To configure or override the hello authentication setting for a given level, configure the `hello-authentication-type` in the `config>router>isis>interface>level` context.

The `no` form of the command disables hello authentication.
Default

no hello-authentication-type — Hello authentication is disabled.

Parameters

password — Specifies simple password (plain text) authentication is required.

message-digest — Specifies MD5 authentication in accordance with RFC2104 (HMAC: Keyed-Hashing for Message Authentication) is required.

hello-interval

Syntax

hello-interval seconds
no hello-interval

Context

config>router>isis>if>level level-number

Description

This command configures the interval in seconds between hello messages issued on this interface at this level.

The no form of the command reverts to the default value.

Default

3 — Hello interval default for the designated intersystem.

9 — Hello interval default for non-designated intersystems.

Parameters

seconds — The hello interval in seconds expressed as a decimal integer.

Values

1 — 20000

hello-multiplier

Syntax

hello-multiplier multiplier
no hello-multiplier

Context

config>router>isis>if>level level-number

Description

This command configures the number of missing hello PDUs from a neighbor after the router declares the adjacency down.

The no form of the command reverts to the default value.

Default

3 — The router can miss up to 3 hello messages before declaring the adjacency down.

Parameters

multiplier — The multiplier for the hello interval expressed as a decimal integer.

Values

2 — 100
interface

Syntax    [no] interface ip-int-name
Context   config>router>isis
Description This command creates the context to configure an IS-IS interface.

When an area is defined, the interfaces belong to that area. Interfaces cannot belong to separate areas.

When the interface is a POS channel, the OSINCP is enabled when the interface is created and removed when the interface is deleted.

The no form of the command removes IS-IS from the interface.

The shutdown command in the config>router>isis>interface context administratively disables IS-IS on the interface without affecting the IS-IS configuration.

Default   no interface — No IS-IS interfaces are defined.

Parameters ip-int-name — Identify the IP interface name created in the config>router>interface context. The IP interface name must already exist.

interface-type

Syntax    interface-type {broadcast | point-to-point}
          no interface-type
Context   config>router>isis>interface ip-int-name
Description This command configures the IS-IS interface type as either broadcast or point-to-point.

Use this command to set the interface type of an Ethernet link to point-to-point to avoid having to carry the designated IS-IS overhead if the link is used as a point-to-point.

If the interface type is not known at the time the interface is added to IS-IS and subsequently the IP interface is bound (or moved) to a different interface type, then this command must be entered manually.

The no form of the command reverts to the default value.

Special Cases SONET — Interfaces on SONET channels default to the point-to-point type.

Ethernet or Unknown — Physical interfaces that are Ethernet or unknown default to the broadcast type.

Default   point-to-point — For IP interfaces on SONET channels.
          broadcast — For IP interfaces on Ethernet or unknown type physical interfaces.

Parameters broadcast — Configures the interface to maintain this link as a broadcast network.
          point-to-point — Configures the interface to maintain this link as a point-to-point link.
**ipv4-routing**

**Syntax**

```
[no] ipv4-routing
```

**Context**

`config>router>isis`

**Description**

This command specifies whether this IS-IS instance supports IPv4.
The `no` form of the command disables IPv4 on the IS-IS instance.

**Default**

`ipv4-routing`

---

**ldp-over-rsvp**

**Syntax**

```
[no] ldp-over-rsvp
```

**Context**

`config>router>isis`

**Description**

This command allows LDP over RSVP processing in IS-IS.
The `no` form of the command disables LDP over RSVP processing.

**Default**

`no ldp-over-rsvp`

---

**iid-tlv-enable**

**Syntax**

```
[no] iid-tlv-enable
```

**Context**

`config>router>isis`

**Description**

This command specifies whether Instance Identifier (IID) TLV has been enabled or disabled for this ISIS instance.

When enabled, each I-IS instance marks its packets with the IID TLV containing its unique 16-bit IID for the routing domain. You should shut/no shut the isis instance to make the change operational.

**Default**

`no iid-tlv-enable`

---

**level**

**Syntax**

```
level level-number
```

**Context**

`config>router>isis`

`config>router>isis>interface ip-int-name`

**Description**

This command creates the context to configure IS-IS Level 1 or Level 2 area attributes.

A router can be configured as a Level 1, Level 2, or Level 1-2 system. A Level 1 adjacency can be established if there is at least one area address shared by this router and a neighbor. A Level 2 adjacency cannot be established over this interface.
Level 1/2 adjacency is created if the neighbor is also configured as Level 1/2 router and has at least one area address in common. A Level 2 adjacency is established if there are no common area IDs.

A Level 2 adjacency is established if another router is configured as Level 2 or a Level 1/2 router with interfaces configured as Level 1/2 or Level 2. Level 1 adjacencies will not established over this interface.

To reset global and/or interface level parameters to the default, the following commands must be entered independently:

```
level> no hello-authentication-key
level> no hello-authentication-type
level> no hello-interval
level> no hello-multiplier
level> no metric
level> no passive
level> no priority
```

**Special Cases**

**Global IS-IS Level** — The `config>router>isis` context configures default global parameters for both Level 1 and Level 2 interfaces.

**IS-IS Interface Level** — The `config>router>isis>interface` context configures IS-IS operational characteristics of the interface at Level 1 and/or Level 2. A logical interface can be configured on one Level 1 and one Level 2. In this case, each level can be configured independently and parameters must be removed independently.

By default an interface operates in both Level 1 and Level 2 modes.

**Default**

level 1 or level 2

**Parameters**  
`level-number` — The IS-IS level number.

**Values**

1, 2

**level-capability**

**Syntax**

```
level-capability {level-1 | level-2 | level-1/2}
no level-capability
```

**Context**

`config>router>isis`
`config>router>isis>interface ip-int-name`

**Description**

This command configures the routing level for an instance of the IS-IS routing process.

An IS-IS router and an IS-IS interface can operate at Level 1, Level 2 or both Level 1 and 2.

Table 13 displays configuration combinations and the potential adjacencies that can be formed.

<table>
<thead>
<tr>
<th>Global Level</th>
<th>Interface Level</th>
<th>Potential Adjacency</th>
</tr>
</thead>
<tbody>
<tr>
<td>L 1/2</td>
<td>L 1/2</td>
<td>Level 1 and/or Level 2</td>
</tr>
<tr>
<td>L 1/2</td>
<td>L 1</td>
<td>Level 1 only</td>
</tr>
</tbody>
</table>

**Table 13: Potential Adjacency Capabilities**
The no form of the command removes the level capability from the configuration.

**Special Cases**

**IS-IS Router** — In the `config>router>isis` context, changing the `level-capability` performs a restart on the IS-IS protocol instance.

**IS-IS Interface** — In the `config>router>isis>interface` context, changing the `level-capability` performs a restart of IS-IS on the interface.

**Default**

`level-1/2`

**Parameters**

- `level-1` — Specifies the router/interface can operate at Level 1 only.
- `level-2` — Specifies the router/interface can operate at Level 2 only.
- `level-1/2` — Specifies the router/interface can operate at both Level 1 and Level 2.

### lsp-pacing-interval

**Syntax**

`lsp-pacing-interval milliseconds`

`no lsp-pacing-interval`

**Context**

`config>router>isis>interface ip-int-name`

**Description**

This command configures the interval between LSP PDUs sent from this interface.

To avoid bombarding adjacent neighbors with excessive data, pace the Link State Protocol Data Units (LSP’s). If a value of zero is configured, no LSP’s are sent from the interface.

The no form of the command reverts to the default value.

**Default**

`100` — LSPs are sent in 100 millisecond intervals.

**Parameters**

- `milliseconds` — The interval in milliseconds that IS-IS LSP’s can be sent from the interface expressed as a decimal integer.

**Values**

- `0` — 65535
IS-IS Commands

lsp-lifetime

Syntax

lsp-lifetime seconds
no lsp-lifetime

Context

config>router>isis

Description

This command sets the time, in seconds, the router wants the LSPs it originates to be considered valid by other routers in the domain.

Each LSP received is maintained in an LSP database until the lsp-lifetime expires unless the originating router refreshes the LSP. By default, each router refreshes its LSP’s every 20 minutes (1200 seconds) so other routers will not age out the LSP.

The LSP refresh timer is derived from this formula: lsp-lifetime/2

The no form of the command reverts to the default value.

Default

1200 — LSPs originated by the router should be valid for 1200 seconds (20 minutes).

Parameters

seconds — The time, in seconds, that the router wants the LSPs it originates to be considered valid by other routers in the domain.

Values

350 — 65535

lsp-mtu-size

Syntax

lsp-mtu-size size
no lsp-mtu-size

Context

config>router>isis

Description

This command configures the LSP MTU size. If the size value is changed from the default using CLI or SNMP, then ISIS must be restarted in order for the change to take effect. This can be done by performing a shutdown command and then a no shutdown command in the config>router>isis context. Note: Using the exec command to execute a configuration file to change the LSP MTU-size from its default value will automatically bounce IS-IS for the change to take effect.

The no form of the command reverts to the default value.

Default

1492

Parameters

size — Specifies the LSP MTU size.

Values

490 — 9190
lsp-wait

**Syntax**
```
lsp-wait [lsp-initial-wait [lsp-second-wait]]
```

**Context**
```
config>router>isis
```

**Description**
This command is used to customize the throttling of IS-IS LSP-generation. Timers that determine when to generate the first, second and subsequent LSPs can be controlled with this command. Subsequent LSPs are generated at increasing intervals of the second `lsp-wait` timer until a maximum value is reached.

**Parameters**
- **lsp-max-wait** — Specifies the maximum interval in seconds between two consecutive occurrences of an LSP being generated.
  - **Values**: 1 — 120
  - **Default**: 5
- **lsp-initial-wait** — Specifies the initial LSP generation delay in seconds.
  - **Values**: 0 — 100
  - **Default**: 0
- **lsp-second-wait** — Specifies the hold time in seconds between the first and second LSP generation.
  - **Values**: 1 — 100
  - **Default**: 1

---

multi-topology

**Syntax**
```
[no] multi-topology
```

**Context**
```
config>router>isis
```

**Description**
This command enables IS-IS multi-topology support.

**Default**
`disabled`

---

multicast-import

**Syntax**
```
[no] multicast-import
```

**Context**
```
config>router>isis
```

**Description**
This command enables the submission of routes into the multicast Route Table Manager (RTM) by IS-IS. The `no` form of the command disables the submission of routes into the multicast RTM.

**Default**
`no multicast-import`
mesh-group

Syntax

mesh-group {value | blocked}
no mesh-group

Context

config>router>isis>interface ip-int-name

Description

This command assigns an interface to a mesh group. Mesh groups limit the amount of flooding that occurs when a new or changed LSP is advertised throughout an area.

All routers in a mesh group should be fully meshed. When LSPs need to be flooded, only a single copy is received rather than a copy per neighbor.

To create a mesh group, configure the same mesh group value for each interface that is part of the mesh group. All routers must have the same mesh group value configured for all interfaces that are part of the mesh group.

To prevent an interface from flooding LSPs, the optional blocked parameter can be specified. Configure mesh groups carefully. It is easy to created isolated islands that do not receive updates as (other) links fail.

The no form of the command removes the interface from the mesh group.

Default

no mesh-group — The interface does not belong to a mesh group.

Parameters

value — The unique decimal integer value distinguishes this mesh group from other mesh groups on this or any other router that is part of this mesh group.

Values

1 — 2000000000

blocked — Prevents an interface from flooding LSPs.

metric

Syntax

metric metric
no metric

Context

config>router>isis>if>level level-number

Description

This command configures the metric used for the level on the interface.

In order to calculate the lowest cost to reach a given destination, each configured level on each interface must have a cost. The costs for each level on an interface may be different.

If the metric is not configured, the default of 10 is used unless reference bandwidth is configured.

The no form of the command reverts to the default value.

Default

10 — A metric of 10 for the level on the interface is used.

Parameters

metric — The metric assigned for this level on this interface.

Values

1 — 16777215
advertise-passive-only

**Syntax**

[no] advertise-passive-only

**Context**

config>router>isis

**Description**

This command enables and disables IS-IS to advertise only prefixes that belong to passive interfaces.

area-id

**Syntax**

[no] area-id area-address

**Context**

config>router>isis

**Description**

This command was previously named the net network-entity-title command. The area-id command allows you to configure the area ID portion of NSAP addresses which identifies a point of connection to the network, such as a router interface, and is called a Network Service Access Point (NSAP). Addresses in the IS-IS protocol are based on the ISO NSAP addresses and Network Entity Titles (NETs), not IP addresses.

A maximum of 3 area addresses can be configured.

NSAP addresses are divided into three parts. Only the area ID portion is configurable.

- **Area ID** — A variable length field between 1 and 13 bytes long. This includes the Authority and Format Identifier (AFI) as the most significant byte and the area ID.
- **System ID** — A six-byte system identification. This value is not configurable. The system ID is derived from the system or router ID.
- **Selector ID** — A one-byte selector identification that must contain zeros when configuring a NET. This value is not configurable. The selector ID is always 00.

The NET is constructed like an NSAP but the selector byte contains a 00 value. NET addresses are exchanged in hello and LSP PDUs. All net addresses configured on the node are advertised to its neighbors.

For Level 1 interfaces, neighbors can have different area IDs, but, they must have at least one area ID (AFI + area) in common. Sharing a common area ID, they become neighbors and area merging between the potentially different areas can occur.

For Level 2 (only) interfaces, neighbors can have different area IDs. However, if they have no area IDs in common, they become only Level 2 neighbors and Level 2 LSPs are exchanged.

For Level 1 and Level 2 interfaces, neighbors can have different area IDs. If they have at least one area ID (AFI + area) in common, they become neighbors. In addition to exchanging Level 2 LSPs, area merging between potentially different areas can occur.

If multiple area-id commands are entered, the system ID of all subsequent entries must match the first area address.

The no form of the command removes the area address.

**Default**

none — No area address is assigned.

**Parameters**

area-address — The 1 — 13-byte address. Of the total 20 bytes comprising the NET, only the first 13 bytes can be manually configured. As few as one byte can be entered or, at most, 13 bytes. If less than 13 bytes are entered, the rest is padded with zeros.
overload

**Syntax**
```
overload [timeout seconds]
no overload
```

**Context**
```
config>router>isis
```

**Description**
This command administratively sets the IS-IS router to operate in the overload state for a specific time period, in seconds, or indefinitely.

During normal operation, the router may be forced to enter an overload state due to a lack of resources. When in the overload state, the router is only used if the destination is reachable by the router and will not used for other transit traffic.

If a time period is specified, the overload state persists for the configured length of time. If no time is specified, the overload state operation is maintained indefinitely.

The `overload` command can be useful in circumstances where the router is overloaded or used prior to executing a `shutdown` command to divert traffic around the router.

The `no` form of the command causes the router to exit the overload state.

**Default**
```
no overload
```

**Parameters**
```
seconds — The time, in seconds, that this router must operate in overload state.
```

Default
```
infinity (overload state maintained indefinitely)
```

**Values**
```
60 — 1800
```

overload-on-boot

**Syntax**
```
overload-on-boot [timeoutseconds]
no overload-on-boot
```

**Context**
```
config>router>isis
```

**Description**
When the router is in an overload state, the router is used only if there is no other router to reach the destination. This command configures the IGP upon bootup in the overload state until one of the following events occur:

1. The timeout timer expires.
2. A manual override of the current overload state is entered with the `config>router>isis>no overload` command.

The `no overload` command does not affect the `overload-on-boot` function.

If no timeout is specified, IS-IS will go into overload indefinitely after a reboot. After the reboot, the IS-IS status will display a permanent overload state:

```
L1 LSDB Overload : Manual on boot (Indefinitely in overload)
L2 LSDB Overload : Manual on boot (Indefinitely in overload)
```

This state can be cleared with the `config>router>isis>no overload` command.
When specifying a timeout value, IS-IS will go into overload for the configured timeout after a reboot. After the reboot, the IS-IS status will display the remaining time the system stays in overload:

L1 LSDB Overload : Manual on boot (Overload Time Left : 17)
L2 LSDB Overload : Manual on boot (Overload Time Left : 17)

The overload state can be cleared before the timeout expires with the `config>router>isis>no overload` command.

The `no` form of the command removes the overload-on-boot functionality from the configuration.

**Default**

no overload-on-boot

Use `show router ospf status` and/or `show router isis status` commands to display the administrative and operational state as well as all timers.

**Parameters**

- **timeout seconds** — Configure the timeout timer for overload-on-boot in seconds.
  - **Values** 60 — 1800

**passive**

**Syntax**

[no] passive

**Context**

`config>router>isis>interface ip-int-name`
`config>router>isis>if>level level-number`

**Description**

This command adds the passive attribute which causes the interface to be advertised as an IS-IS interface without running the IS-IS protocol. Normally, only interface addresses that are configured for IS-IS are advertised as IS-IS interfaces at the level that they are configured.

When the passive mode is enabled, the interface or the interface at the level ignores ingress IS-IS protocol PDUs and will not transmit IS-IS protocol PDUs.

The `no` form of the command removes the passive attribute.

**Special Cases**

- **Service Interfaces** — Service interfaces (defined using the service-prefix command in `config>router`) are passive by default.
- **All other Interfaces** — All other interfaces are not passive by default.

**Default**

- **passive** — Service interfaces are passive.
- **no passive** — All other interfaces are not passive.

**preference**

**Syntax**

`preference preference`

`no preference`

**Context**

`config>router>isis>level level-number`

**Description**

This command configures the preference level of either IS-IS Level 1 or IS-IS Level 2 internal routes. By default, the preferences are listed in the table below.
A route can be learned by the router by different protocols, in which case, the costs are not comparable. When this occurs, the preference is used to decide to which route will be used.

Different protocols should not be configured with the same preference, if this occurs the tiebreaker is per the default preference table as defined in the table below. If multiple routes are learned with an identical preference using the same protocol, the lowest cost route is used. If multiple routes are learned with an identical preference using the same protocol and the costs (metrics) are equal, then the decision what route to use is determined by the configuration of the `ecmp` in the `config>router` context.

### Default

Default preferences are listed in the following table:

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Preference</th>
<th>Configurable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct attached</td>
<td>0</td>
<td>No</td>
</tr>
<tr>
<td>Static-route</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF internal routes</td>
<td>10</td>
<td>No</td>
</tr>
<tr>
<td>IS-IS level 1 internal</td>
<td>15</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 2 internal</td>
<td>18</td>
<td>Yes</td>
</tr>
<tr>
<td>OSPF external</td>
<td>150</td>
<td>Yes</td>
</tr>
<tr>
<td>IS-IS level 1 external</td>
<td>160</td>
<td>Yes*</td>
</tr>
<tr>
<td>IS-IS level 2 external</td>
<td>165</td>
<td>Yes*</td>
</tr>
</tbody>
</table>

* External preferences are changed using the `external-preference` command in the `config>router>isis>level level-number` context.

### Parameters

`preference` — The preference for external routes at this level expressed as a decimal integer.

**Values**

1 — 255

### priority

#### Syntax

`priority number`

`no priority`

#### Context

`config>router>isis>if>level level-number`

#### Description

This command configures the priority of the IS-IS router interface for designated router election on a multi-access network.

This priority is included in hello PDUs transmitted by the interface on a multi-access network. The router with the highest priority is the preferred designated router. The designated router is responsible for sending LSPs with regard to this network and the routers that are attached to it.

The `no` form of the command reverts to the default value.

**Default**

64
Parameters  

*number* — The priority for this interface at this level.

**Values**  

0 — 127

### psnp-authentication

**Syntax**  

```
[no] psnp-authentication
```

**Context**  

```
config>router>isis
config>router>isis>level
```

**Description**  

This command enables authentication of individual ISIS packets of partial sequence number PDU (PSNP) type. The *no* form of the command suppresses authentication of PSNP packets.

### reference-bandwidth

**Syntax**  

```
reference-bandwidth reference-bandwidth
no reference-bandwidth
```

**Context**  

```
config>router>isis
```

**Description**  

This command configures the reference bandwidth that provides the basis of bandwidth relative costing. In order to calculate the lowest cost to reach a specific destination, each configured level on each interface must have a cost. If the reference bandwidth is defined, then the cost is calculated using the following formula:

```
cost = reference-bandwidth / bandwidth
```

If the reference bandwidth is configured as 10 Gigabits (10,000,000,000), a 100 M/bps interface has a default metric of 100. In order for metrics in excess of 63 to be configured, wide metrics must be deployed. (See *wide-metrics-only* in the `config>router>isis` context.)

If the reference bandwidth is not configured, then all interfaces have a default metric of 10.

The *no* form of the command reverts to the default value.

**Default**  

*no reference-bandwidth* — No reference bandwidth is defined. All interfaces have a metric of 10.

**Parameters**  

*reference-bandwidth* — The reference bandwidth in kilobits per second expressed as a decimal integer.
rsvp-shortcut

**Syntax**  

```plaintext
[no] rsvp-shortcut
```

**Context**  

`config>router>isis`

**Description**  

This command enables the use of an RSVP-TE shortcut for resolving IGP routes by IS-IS or OSPF routing protocols.

This command instructs IS-IS or OSPF to include RSVP LSPs originating on this node and terminating on the router-id of a remote node as direct links with a metric equal to the operational metric provided by MPLS.

When `rsvp-shortcut` is enabled at the IGP instance level, all RSVP LSPs originating on this node are eligible by default as long as the destination address of the LSP, as configured in `configure>router>mpls>lsp>to`, corresponds to a router-id of a remote node. RSVP LSPs with a destination address corresponding to an interface address of a remote node are automatically not considered by IS-IS or OSPF. The user can however exclude a specific RSVP LSP from being used as a shortcut for resolving IGP routes by entering the command `config>router>mpls>lsp>no igp-shortcut`.

Also, the SPF in OSPF or IS-IS will only use RSVP LSPs as IGP shortcuts or as endpoints for LDP-over-RSV. These applications of RSVP LSPs are mutually exclusive at the IGP instance level. If the user enabled both options at the IGP instance level, then the shortcut application takes precedence when the LSP level configuration has both options enabled.

When an IPv4 packet is received on an ingress network interface, a subscriber IES interface, or a regular IES interface, the lookup of the packet in RTM will result in the resolution of the packet to an RSVP LSP if all the following conditions are satisfied:

- RSVP shortcut is enabled on the IGP routing protocol which has a route for the packet's destination address.
- SPF has pre-determined that the IGP path cost using the RSVP LSP shortcut is the best.

In this case, the packet is sent labeled with the label stack corresponding to the NHLFE of the RSVP LSP.

The failure of an RSVP LSP shortcut or of a local interface triggers a full SPF computation which may result in installing a new route over another RSVP LSP shortcut or a regular IP next-hop.

When ECMP is enabled and multiple equal-cost paths exist for the IGP route, the ingress IOM will spray the packets for this route based on hashing routine currently supported for IPv4 packets. Spraying will be performed across a regular IP next-hop and across an RSVP shortcut next-hop as long as the IP path does not go over the tail-end of the RSVP LSP.

The no form of this command disables the resolution of IGP routes using RSVP shortcuts.

**Default**  

`no rsvp-shortcut`
advertise-tunnel-links

Syntax: [no] advertise-tunnel-links

Context: config>router>isis

Description: This command enables the advertisement of RSVP LSP shortcuts into IGP similar to regular links so that other routers in the network can include them in their SPF computations. An LSP must exist in the reverse direction in order for the advertised link to pass the bi-directional link check and be usable by other routers in the network. However, this is not required for the node which originates the LSP.

The LSP is advertised as an unnumbered point-to-point link and the link LSP/LSA has no Traffic Engineering opaque sub-TLVs per RFC 3906.

The no form of this command disables the advertisement of RSVP LSP shortcuts into IGP.

Default: no advertise-tunnel-links

retransmit-interval

Syntax: retransmit-interval seconds
no retransmit-interval

Context: config>router>isis>interface ip-int-name

Description: This command configures the minimum time between LSP PDU retransmissions on a point-to-point interface.

The no form of the command reverts to the default value.

Default: 100

Parameters: seconds — The interval in seconds that IS-IS LSPs can be sent on the interface.

Values: 1 — 65535

spf-wait

Syntax: [no] spf-wait spf-wait [spf-initial-wait [spf-second-wait]]

Context: config>router>isis

Description: This command defines the maximum interval between two consecutive SPF calculations in seconds. Timers that determine when to initiate the first, second and subsequent SPF calculations after a topology change occurs can be controlled with this command. Subsequent SPF runs (if required) will occur at exponentially increasing intervals of the spf-second-wait interval. For example, if the spf-second-wait interval is 1000, then the next SPF will run after 2000 milliseconds, and then next SPF will run after 4000 milliseconds, etc., until it reaches the spf-wait value. The SPF interval will stay at spf-wait value until there are no more SPF runs scheduled in that interval. After a full interval without any SPF runs, the SPF interval will drop back to spf-initial-wait.
IS-IS Commands

Default

Parameters

- no spf-wait
- spf-wait — Specifies the maximum interval in seconds between two consecutive spf calculations.
  - Values: 1 — 120
  - Default: 10
- spf-initial-wait — Specifies the initial SPF calculation delay in milliseconds after a topology change.
  - Values: 10 — 100000
  - Default: 1000
- spf-second-wait — Specifies the hold time in milliseconds between the first and second SPF calculation.
  - Values: 1 — 100000
  - Default: 1000

summary-address

Syntax

- summary-address {ip-prefix/mask | ip-prefix [netmask]} level [tag tag]
- no summary-address {ip-prefix/mask | ip-prefix [netmask]}

Context

config>router>isis

Description

This command creates summary-addresses.

Default

none

Parameters

- ip-prefix/mask — Specifies information for the specified IP prefix and mask length.
  - Values: ipv4-prefix: a.b.c.d (host bits must be 0)
    ipv4-prefix-length: 0 — 32
- netmask — The subnet mask in dotted decimal notation.
  - Values: 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)
- level — Specifies IS-IS level area attributes.
  - Values: level-1, level-2, level-1/2
- tag tag — Assigns an OSPF, RIP or ISIS tag to routes matching the entry.
  - Values: Accepts decimal or hex formats:
    OSPF and ISIS: [0x0..0xFFFFFFFF]H
    RIP: [0x0..0xFFFF]H
suppress-default

Syntax  [no] suppress-default
Context  config>router>isis
Description  This command enables or disables IS-IS to suppress the installation of default routes.

traffic-engineering

Syntax  [no] traffic-engineering
Context  config>router>isis
Description  This command configures traffic-engineering and determines if IGP shortcuts are required.
Default  disabled

unicast-import-disable

Syntax  [no] unicast-import-disable
Context  config>router>isis
Description  This command allows one IGP to import its routes into RPF RTM while another IGP imports routes only into the unicast RTM. Import policies can redistribute routes from an IGP protocol into the RPF RTM (the multicast routing table). By default, the IGP routes will not be imported into RPF RTM as such an import policy must be explicitly configured.
Default  disabled

wide-metrics-only

Syntax  [no] wide-metrics-only
Context  config>router>isis>level level-number
Description  This command enables the exclusive use of wide metrics in the LSPs for the level number. Narrow metrics can have values between 1 and 63. IS-IS can generate two TLVs, one for the adjacency and one for the IP prefix. In order to support traffic engineering, wider metrics are required. When wide metrics are used, a second pair of TLVs are added, again, one for the adjacency and one for the IP prefix.
By default, both sets of TLVs are generated. When wide-metrics-only is configured, IS-IS only generates the pair of TLVs with wide metrics for that level.
The no form of the command reverts to the default value.
Show Commands

isis

Syntax  isis [isis-instance]
Context  show>router
Description  This command displays information for a specified IS-IS instance.
Parameters  instance-id — Specifies the instance ID for an IS-IS instance.
  Values  1–31
  Default  0

adjacency

Syntax  adjacency [ip-address | ip-int-name | nbr-system-id] [detail]
Context  show>router>isis
Description  This command displays information regarding IS-IS neighbors. When no ip-address, ip-int-name, or nbr-system-id are specified, then all adjacencies display.
Parameters  ip-address — When specified, only adjacencies with that interface display.
  Values  ipv4-address: a.b.c.d (host bits must be 0)
  ip-int-name — When specified, only adjacencies with that interface display.
  nbr-system-id — When specified, only the adjacency with that ID displays.
  detail — All output displays in the detailed format.

Output  Standard and Detailed IS-IS Adjacency Output — The following table describes the standard and detailed command output fields for an IS-IS adjacency.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface name associated with the neighbor.</td>
</tr>
<tr>
<td>System-id</td>
<td>Neighbor’s system ID.</td>
</tr>
<tr>
<td>Level</td>
<td>1-L1 only, 2-L2 only, 3-L1 and L2.</td>
</tr>
<tr>
<td>State</td>
<td>Up, down, new, one-way, initializing, or rejected.</td>
</tr>
<tr>
<td>Hold</td>
<td>Hold time remaining for the adjacency.</td>
</tr>
<tr>
<td>SNPA</td>
<td>Subnetwork point of attachment, MAC address of the next hop.</td>
</tr>
</tbody>
</table>
Sample Output

*A:Dut-A# show router isis adjacency

ISIS Adjacency

<table>
<thead>
<tr>
<th>System ID</th>
<th>Usage</th>
<th>State</th>
<th>Hold</th>
<th>Interface</th>
<th>MT Enab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dut-B</td>
<td>L1</td>
<td>Up</td>
<td>2</td>
<td>ip-3FFE::A0A:101</td>
<td>Yes</td>
</tr>
<tr>
<td>Dut-B</td>
<td>L2</td>
<td>Up</td>
<td>2</td>
<td>ip-3FFE::A0A:101</td>
<td>Yes</td>
</tr>
<tr>
<td>Dut-F</td>
<td>L1L2</td>
<td>Up</td>
<td>5</td>
<td>ies-1-3FFE::A0A:1501</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Adjacencies : 3

*A:Dut-A#

*A:ALA-A# show router isis adjacency 180.0.7.12

ISIS Adjacency

<table>
<thead>
<tr>
<th>System ID</th>
<th>Usage</th>
<th>State</th>
<th>Hold</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>asbr_east</td>
<td>L2</td>
<td>Up</td>
<td>25</td>
<td>if2/5</td>
</tr>
</tbody>
</table>

Adjacencies : 1

*A:ALA-A#

*A:ALA-A# show router isis adjacency if2/5

ISIS Adjacency

<table>
<thead>
<tr>
<th>System ID</th>
<th>Usage</th>
<th>State</th>
<th>Hold</th>
<th>Interface</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit type</td>
<td>Level on the interface L1, L2, or both.</td>
</tr>
<tr>
<td>Expires In</td>
<td>Number of seconds until adjacency expires.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority to become designated router.</td>
</tr>
<tr>
<td>Up/down transitions</td>
<td>Number of times neighbor state has changed.</td>
</tr>
<tr>
<td>Event</td>
<td>Event causing last transition.</td>
</tr>
<tr>
<td>Last transition</td>
<td>Time since last transition change.</td>
</tr>
<tr>
<td>Speaks</td>
<td>Supported protocols (only IP).</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of neighbor.</td>
</tr>
<tr>
<td>MT enab</td>
<td>Yes — The neighbor is advertising at least 1 non MTID#0.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit type</td>
<td>Level on the interface L1, L2, or both.</td>
</tr>
<tr>
<td>Expires In</td>
<td>Number of seconds until adjacency expires.</td>
</tr>
<tr>
<td>Priority</td>
<td>Priority to become designated router.</td>
</tr>
<tr>
<td>Up/down transitions</td>
<td>Number of times neighbor state has changed.</td>
</tr>
<tr>
<td>Event</td>
<td>Event causing last transition.</td>
</tr>
<tr>
<td>Last transition</td>
<td>Time since last transition change.</td>
</tr>
<tr>
<td>Speaks</td>
<td>Supported protocols (only IP).</td>
</tr>
<tr>
<td>IP address</td>
<td>IP address of neighbor.</td>
</tr>
<tr>
<td>MT enab</td>
<td>Yes — The neighbor is advertising at least 1 non MTID#0.</td>
</tr>
</tbody>
</table>
asbr_east                        L2    Up    20   if2/5

Adjacencies : 1

*A:ALA-A#

*A:Dut-A# show router isis adjacency detail

ISIS Adjacency

SystemID      : Dut-B                        SNPA      : 20:81:01:01:00:01
Interface     : ip-3FFE::A0A:101            Up Time   : 0d 00:56:10
State         : Up                            Priority  : 64
Nbr Sys Typ   : L1                            L. Circ Typ : L1
Hold Time     : 2                             Max Hold  : 2
Adj Level     : L1                            MT Enabled : Yes
IPv4 Neighbor : 10.10.1.2
Restart Support: Disabled
Restart Status : Not currently being helped
Restart Suppressed : Disabled
Number of Restarts: 0
Last Restart at : Never

SystemID      : Dut-F                        SNPA      : 00:00:00:00:00:00
Interface     : ies-1-3FFE::A0A:1501          Up Time   : 0d 01:18:34
State         : Up                            Priority  : 0
Nbr Sys Typ   : L1L2                          L. Circ Typ : L1L2
Hold Time     : 5                             Max Hold  : 6
Adj Level     : L1L2                          MT Enabled : Yes
IPv6 Neighbor : FE80::2285:FFFF:FE00:0
IPv4 Neighbor : 10.10.21.6
Restart Support: Disabled
Restart Status : Not currently being helped
Restart Suppressed : Disabled
Number of Restarts: 0
Last Restart at : Never

*A:Dut-A#
Show Commands

A:Dut-A# show router isis status

===============================================================================
ISIS Status
===============================================================================
System Id            : 0100.2000.1001
Admin State          : Up
Ipv4 Routing         : Enabled
Level Capability     : L2
Authentication Check : True
Authentication Type  : None
HELLO-Authentication : Enabled
PSNP-Authentication  : Enabled
Traffic Engineering  : Enabled
Graceful Restart     : Disabled
GR Helper Mode       : Disabled
LSP Lifetime         : 1200
LSP Wait             : 1 sec (Max)   1 sec (Initial)   1 sec (Second)
Adjacency Check      : loose
L1 Auth Type         : none
L2 Auth Type         : none
L1 CSNP-Authentication: Enabled
L1 HELLO-Authentication: Enabled
L1 PSNP-Authentication: Enabled
L1 Preference        : 15
L2 Preference        : 18
L1 Ext. Preference   : 160
L2 Ext. Preference   : 165
L1 Wide Metrics      : Disabled
L2 Wide Metrics      : Enabled
L1 LSDB Overload     : Disabled
L2 LSDB Overload     : Disabled
L1 LSPs              : 0
L2 LSPs              : 15
SPF Wait             : 1 sec (Max)   10 ms (Initial)   10 ms (Second)
Export Policies      : None
Area Addresses       : 49.0001

* indicates that the corresponding row element may have been truncated.
A:Dut-A#

database

Syntax    database [system-id | lsp-id] [detail] [level level]
Context   show>router>isis
Description This command displays the entries in the IS-IS link state database.
Parameters system-id — Only the LSPs related to that system-id are listed. If no system-id or lsp-id are specified, all database entries are listed.
lsp-id — Only the specified LSP (hostname) is listed. If no system-id or lsp-id are specified, all database entries are listed.
**detail** — All output is displayed in the detailed format.

**level level** — Only the specified IS-IS protocol level attributes are displayed.

**Output IS-IS Database Output** — The following table describes the IS-IS database output.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSP ID</td>
<td>LSP IDs are auto-assigned by the originating IS-IS node. The LSP ID is comprised of three sections. The first 6 bytes is the system ID for that node, followed by a single byte value for the pseudonode generated by that router, then finally, a fragment byte which starts at zero. For example, if a router’s system ID is 1800.0000.0029, the first LSP ID is 1800.0000.0029.00-00. If there are too many routes, LSP ID 1800.0000.0029.00-01 is created to contain the excess routes. If the router is the Designated Intermediate System (DIS) on a broadcast network, a pseudo-node LSP is created. Usually the internal circuit ID is used to determine the ID assigned to the pseudonode. For instance, for circuit 4, a LSP pseudonode with ID 1800.0000.0029.04-00 is created. The SR-OS node learns hostnames and uses the hostname in place of the system ID. An example of LDP IDs are: acc_arl.00-00 acc_arl.00-01 acc_arl.04-00</td>
</tr>
<tr>
<td>Sequence</td>
<td>The sequence number of the LSP that allows other systems to determine if they have received the latest information from the source.</td>
</tr>
<tr>
<td>Checksum</td>
<td>The checksum of the entire LSP packet.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Amount of time, in seconds, that the LSP remains valid.</td>
</tr>
<tr>
<td>Attributes</td>
<td>OV — The overload bit is set.</td>
</tr>
<tr>
<td></td>
<td>L1 — Specifies a Level 1 IS type.</td>
</tr>
<tr>
<td></td>
<td>L2 — Specifies a Level 2 IS type.</td>
</tr>
<tr>
<td></td>
<td>ATT — The attach bit is set. When this bit is set, the router can also act as a Level 2 router and can reach other areas.</td>
</tr>
<tr>
<td>LSP Count</td>
<td>A sum of all the configured Level 1 and Level 2 LSPs.</td>
</tr>
<tr>
<td>LSP ID</td>
<td>Displays a unique identifier for each LSP composed of SysID, Pseudonode ID and LSP name.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>Displays the remaining time until the LSP expires.</td>
</tr>
<tr>
<td>Version</td>
<td>Displays the version/protocol ID extension. This value is always set to 1.</td>
</tr>
<tr>
<td>Pkt Type</td>
<td>Displays the PDU type number.</td>
</tr>
</tbody>
</table>
**Show Commands**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pkt Ver</td>
<td>Displays the version/protocol ID extension. This value is always set to 1.</td>
</tr>
<tr>
<td>Max Area</td>
<td>Displays the maximum number of area addresses supported.</td>
</tr>
<tr>
<td>Sys ID Len</td>
<td>Displays the length of the system ID field (0 or 6 for 6 digits).</td>
</tr>
<tr>
<td>Use Len</td>
<td>The actual length of the PDU.</td>
</tr>
<tr>
<td>Alloc Len</td>
<td>The amount of memory space allocated for the LSP.</td>
</tr>
<tr>
<td>Area Address</td>
<td>Displays the area addresses to which the router is connected.</td>
</tr>
<tr>
<td>Supp Protocols</td>
<td>Displays the data protocols that are supported.</td>
</tr>
<tr>
<td>IS-Hostname</td>
<td>The name of the router originating the LSP.</td>
</tr>
<tr>
<td>Virtual Flag</td>
<td>0 — Level 1 intermediate systems report this octet as 0 to all neighbors.</td>
</tr>
<tr>
<td></td>
<td>1 — Indicates that the path to a neighbor is a Level 2 virtual path used to repair an area partition.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>Displays the routers running interfaces to which the router is connected.</td>
</tr>
<tr>
<td>Internal Reach</td>
<td>Displays a 32-bit metric. A bit is added for the ups and downs resulting from Level 2 to Level 1 route-leaking.</td>
</tr>
<tr>
<td>IP Prefix</td>
<td>Displays the IP addresses that the router knows about by externally-originated interfaces.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Displays a routing metric used in the IS-IS link-state calculation.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
*A:ALA-A# show router isis database

ISIS Database

LSP ID Sequence Checksum Lifetime Attributes
Displaying Level 1 database
  abr_dfw.00-00 0x50 0x164f 603 L1L2
  Level (1) LSP Count : 1
Displaying Level 2 database
  asbr_east.00-00 0x53 0xe3f5 753 L1L2 0x57 0x94ff 978 L1L2
  abr_dfw.03-00 0x50 0x14f1 614 L1L2
  Level (2) LSP Count : 3

*A:ALA-A#
```
*A:Dut-B# show router isis database Dut-A.00-00 detail

Displaying Level 1 database

Level 1 LSP Count : 0

Displaying Level 2 database

LSP ID : Dut-A.00-00 Level : L2
Sequence : 0x6 Checksum : 0xb7c4 Lifetime : 1153
Version : 1 Pkt Type : 20 Pkt Ver : 1
Attributes: L1L2 Max Area : 3
SysID Len : 6 Used Len : 311 Alloc Len : 311

TLVs :

Area Addresses:
  Area Address : (2) 30.31
Supp Protocols:
  Protocols : IPv4
IS-Hostname : Dut-A
Router ID :
  Router ID : 10.20.1.1
I/F Addresses :
  I/F Address : 10.20.1.1
  I/F Address : 10.10.1.1
  I/F Address : 10.10.2.1
TE IS Nbrs :
  Nbr : Dut-B.01
Default Metric : 1000
Sub TLV Len : 98
IF Addr : 10.10.1.1
MaxLink BW: 100000 kbps
Resvble BW: 100000 kbps
Unresvld BW:
  BW[0] : 10000 kbps
  BW[1] : 40000 kbps
  BW[7] : 10000 kbps
Admin Grp : 0x0
TE Metric : 1000
SUBTLV BW CONSTS : 8
  BW Model : 1
  BC[0]: 10000 kbps
  BC[1]: 0 kbps
  BC[2]: 40000 kbps
  BC[3]: 0 kbps
  BC[4]: 0 kbps
  BC[5]: 50000 kbps
  BC[6]: 0 kbps
  BC[7]: 0 kbps
TE IP Reach :
hostname

Syntax hostname

Context show>router>isis

Description This command displays the hostname database. There are no options or parameters.

Output IS-IS Hostname Output — The following table describes output fields for IS-IS hostname output.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System-id</td>
<td>System identifier mapped to hostname.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname for the specific system-id.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of entry (static or dynamic).</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-A# show router isis hostname

<table>
<thead>
<tr>
<th>System Id</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800.0000.0002</td>
<td>core_west</td>
</tr>
<tr>
<td>1800.0000.0005</td>
<td>core_east</td>
</tr>
<tr>
<td>1800.0000.0008</td>
<td>asbr_west</td>
</tr>
<tr>
<td>1800.0000.0009</td>
<td>asbr_east</td>
</tr>
<tr>
<td>1800.0000.0010</td>
<td>abr_sjc</td>
</tr>
<tr>
<td>1800.0000.0011</td>
<td>abr_lax</td>
</tr>
<tr>
<td>1800.0000.0012</td>
<td>abr_nyc</td>
</tr>
<tr>
<td>1800.0000.0013</td>
<td>abr_dfw</td>
</tr>
<tr>
<td>1800.0000.0015</td>
<td>dist_oak</td>
</tr>
<tr>
<td>1800.0000.0018</td>
<td>dist_nj</td>
</tr>
<tr>
<td>1800.0000.0020</td>
<td>acc_nj</td>
</tr>
<tr>
<td>1800.0000.0021</td>
<td>acc_ri</td>
</tr>
<tr>
<td>1800.0000.0027</td>
<td>dist_arl</td>
</tr>
<tr>
<td>1800.0000.0028</td>
<td>dist_msq</td>
</tr>
<tr>
<td>1800.0000.0029</td>
<td>acc_arl</td>
</tr>
</tbody>
</table>
interface

Syntax  interface [ip-int-name | ip-address] [detail]

Context  show>router>isis

Description  This command shows IS-IS interface information. When no ip-addr or the ip-int-name is specified, all interfaces are listed.

Parameters  ip-address — Only displays the interface information associated with the specified IP address.

  Values  ipv4-address  a.b.c.d (host bits must be 0)

ip-int-name — Only displays the interface information associated with the specified IP interface name.

  detail — All output is given in the detailed format.

Output  IS-IS Interface Output — The following table describes IS-IS interface output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface name.</td>
</tr>
<tr>
<td>Level</td>
<td>Specifies the interface level (1, 2, or 1 and 2).</td>
</tr>
<tr>
<td>CirID</td>
<td>Specifies the circuit identifier.</td>
</tr>
<tr>
<td>Oper State</td>
<td>Up — The interface is operationally up.</td>
</tr>
<tr>
<td></td>
<td>Down — The interface is operationally down.</td>
</tr>
<tr>
<td>L1/L2 Metric</td>
<td>Interface metric for Level 1 and Level 2, if none are set to 0.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-A# show router isis interface

<table>
<thead>
<tr>
<th>Interface</th>
<th>Level</th>
<th>CirID</th>
<th>Oper State</th>
<th>L1/L2 Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>L1L2</td>
<td>1</td>
<td>Up</td>
<td>10/10</td>
</tr>
<tr>
<td>if2/1</td>
<td>L2</td>
<td>8</td>
<td>Up</td>
<td>~/10</td>
</tr>
<tr>
<td>if2/2</td>
<td>L1</td>
<td>5</td>
<td>Up</td>
<td>10/~</td>
</tr>
<tr>
<td>if2/3</td>
<td>L1</td>
<td>6</td>
<td>Up</td>
<td>10/~</td>
</tr>
<tr>
<td>if2/4</td>
<td>L1</td>
<td>7</td>
<td>Up</td>
<td>10/~</td>
</tr>
<tr>
<td>if2/5</td>
<td>L2</td>
<td>2</td>
<td>Up</td>
<td>~/10</td>
</tr>
<tr>
<td>lag-1</td>
<td>L2</td>
<td>3</td>
<td>Up</td>
<td>~/10</td>
</tr>
<tr>
<td>if2/8</td>
<td>L2</td>
<td>4</td>
<td>Up</td>
<td>~/10</td>
</tr>
</tbody>
</table>

Interfaces : 8
## Show Commands

```plaintext
A:ALA-A#

A:SetupCLI# show router isis interface detail

### ISIS Interfaces

<table>
<thead>
<tr>
<th>Interface</th>
<th>Oper State</th>
<th>Auth Type</th>
<th>Circuit Id</th>
<th>Type</th>
<th>Admin Groups</th>
<th>Ldp Sync</th>
<th>Ldp Timer State</th>
<th>Route Tag</th>
<th>Level</th>
<th>Level Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>Up</td>
<td>None</td>
<td>1</td>
<td>Pt-to-Pt</td>
<td></td>
<td></td>
<td></td>
<td>4294967295</td>
<td>2</td>
<td>L2</td>
</tr>
<tr>
<td>ip_if_1</td>
<td>Down</td>
<td>None</td>
<td>5</td>
<td>Pt-to-Pt</td>
<td></td>
<td></td>
<td></td>
<td>4294967295</td>
<td>1</td>
<td>L1L2</td>
</tr>
<tr>
<td>LOA1</td>
<td>Down</td>
<td>Password</td>
<td>64</td>
<td>Pt-to-Pt</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>L1L2</td>
</tr>
</tbody>
</table>
```

---

*Note: The output is truncated for brevity. The full command output would include more detailed information.*
**IS-IS**

<table>
<thead>
<tr>
<th>Auth Type</th>
<th>: None</th>
<th>Auth State</th>
<th>: Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Circuit Id</td>
<td>: 49</td>
<td>Retransmit Int.</td>
<td>: 5</td>
</tr>
<tr>
<td>Type</td>
<td>: Broadcast</td>
<td>LSP Pacing Int.</td>
<td>: 100</td>
</tr>
<tr>
<td>CSNP Int.</td>
<td>: 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mesh Group</td>
<td>: Inactive</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bfd Enabled</td>
<td>: No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Te Metric</td>
<td>: 0</td>
<td>Te State</td>
<td>: Down</td>
</tr>
<tr>
<td>Admin Groups</td>
<td>: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ldp Sync</td>
<td>: outOfService</td>
<td>Ldp Sync Wait</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Ldp Timer State</td>
<td>: Disabled</td>
<td>Ldp Tm Left</td>
<td>: 0</td>
</tr>
<tr>
<td>Route Tag</td>
<td>: None</td>
<td>LFA</td>
<td>: Excluded</td>
</tr>
<tr>
<td>Level</td>
<td>: 1</td>
<td>Adjacencies</td>
<td>: 0</td>
</tr>
<tr>
<td>Desg. IS</td>
<td>: 0000.0000.0000</td>
<td>Metric</td>
<td>: 1000</td>
</tr>
<tr>
<td>Auth Type</td>
<td>: None</td>
<td>Hello Timer</td>
<td>: 9</td>
</tr>
<tr>
<td>Hello Timer</td>
<td>: 9</td>
<td>Hello Mult.</td>
<td>: 3</td>
</tr>
<tr>
<td>Priority</td>
<td>: 64</td>
<td>IPv6-Ucast-Met</td>
<td>: 1000</td>
</tr>
<tr>
<td>Passive</td>
<td>: No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level</td>
<td>: 2</td>
<td>Adjacencies</td>
<td>: 0</td>
</tr>
<tr>
<td>Desg. IS</td>
<td>: 0000.0000.0000</td>
<td>Metric</td>
<td>: 1000</td>
</tr>
<tr>
<td>Auth Type</td>
<td>: None</td>
<td>Hello Timer</td>
<td>: 9</td>
</tr>
<tr>
<td>Hello Timer</td>
<td>: 9</td>
<td>Hello Mult.</td>
<td>: 3</td>
</tr>
<tr>
<td>Priority</td>
<td>: 64</td>
<td>IPv6-Ucast-Met</td>
<td>: 1000</td>
</tr>
<tr>
<td>Passive</td>
<td>: No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Ifa-coverage

**Syntax**

`ifa-coverage`

**Context**

`show>router>isis`

**Description**

This command displays IS-IS LFA coverage information.

**Sample Output**

```
*A:SR# show router isis ifa-coverage
LFA Coverage
Topology  Level Node IPv4
-----------------------------------------------
IPV4 Unicast L1 4/4(100%) 826/826(100%)
IPV4 Unicast L2 2/2(100%) 826/826(100%)
IPV6 Unicast L1 3/3(100%) 0/0(0%)
IPV6 Unicast L2 0/0(0%) 0/0(0%)
-----------------------------------------------
*A:SR#
*A:SRR>config>router>isis# show router isis ifa-coverage
LFA Coverage
Topology  Level Node IPv4 IPv6
-----------------------------------------------
```

**7450 ESS OS Routing Protocols Guide**
neighbor

Syntax neighbor

Context show>router>isis

Description This command displays neighboring route information in the IS-IS route table.

Sample Output

A:linus-212# show router isis neighbor

Topology Table

Node Interface Nexthop

IS-IS IP paths (MT-ID 0), Level 1
linus-211.00 ab linus-211
linus-216.00 ab linus-211
linus-216.01 ab linus-211

IS-IS IP paths (MT-ID 0), Level 2
linus-211.00 ab linus-211
linus-216.00 ab linus-211
linus-216.01 ab linus-211

routes

Syntax routes [ mt mt-id-number | alternative | ip-prefix[/prefix-length] ]

Context show>router>isis

Description This command displays the routes in the IS-IS route table.

Parameters

ipv4-unicast — Displays IPv4 unicast parameters.
mt mt-id-number — Displays multi-topology parameters.

Values 0, 2

alternative — Displays LFA details.
Output

IS-IS Route Output — The following table describes IS-IS route output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>The route prefix and mask.</td>
</tr>
<tr>
<td>Metric MT</td>
<td>The route’s metric.</td>
</tr>
<tr>
<td>Lvl/Type</td>
<td>Specifies the level (1 or 2) and the route type, Internal (Int) or External (Ext).</td>
</tr>
<tr>
<td>Version</td>
<td>SPF version that generated route.</td>
</tr>
<tr>
<td>NextHop</td>
<td>System ID of nexthop, give hostname if possible.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname for the specific system-id.</td>
</tr>
</tbody>
</table>

Sample Output

*A:Dut-B# show router isis routes

Route Table

<table>
<thead>
<tr>
<th>Prefix [Flags]</th>
<th>Metric</th>
<th>Lvl/Type</th>
<th>Ver.</th>
<th>SysID/Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.1.2/32</td>
<td>0</td>
<td>Int.</td>
<td>3</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.20.1.3/32</td>
<td>0</td>
<td>Int.</td>
<td>3</td>
<td>Dut-C</td>
</tr>
<tr>
<td>10.20.1.5/32</td>
<td>20</td>
<td>Int.</td>
<td>2</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.20.1.6/32</td>
<td>20</td>
<td>Int.</td>
<td>3</td>
<td>Dut-D</td>
</tr>
<tr>
<td>10.20.3.0/24</td>
<td>10</td>
<td>Int.</td>
<td>3</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.20.4.0/24</td>
<td>10</td>
<td>Int.</td>
<td>3</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.20.5.0/24</td>
<td>20</td>
<td>Int.</td>
<td>2</td>
<td>Dut-C</td>
</tr>
<tr>
<td>10.20.6.0/24</td>
<td>20</td>
<td>Int.</td>
<td>4</td>
<td>Dut-D</td>
</tr>
<tr>
<td>10.20.9.0/24</td>
<td>20</td>
<td>Int.</td>
<td>3</td>
<td>Dut-D</td>
</tr>
<tr>
<td>10.20.10.0/24</td>
<td>30</td>
<td>Int.</td>
<td>3</td>
<td>Dut-C</td>
</tr>
<tr>
<td>10.20.3.3</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Routes : 11
Flags: L = LFA nexthop available

*A:Dut-B# show router isis routes alternative

*A:Dut-B#
### Route Table

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Metric</th>
<th>Lvl/Typ</th>
<th>Ver.</th>
<th>SysID/Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.1.2/32</td>
<td>10</td>
<td>2/Int.</td>
<td>2</td>
<td>Dut-C</td>
</tr>
<tr>
<td>10.20.3.3</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.4/32</td>
<td>10</td>
<td>2/Int.</td>
<td>3</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.20.4.4</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.3.3 (lfa)</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.5/32</td>
<td>20</td>
<td>2/Int.</td>
<td>3</td>
<td>Dut-D</td>
</tr>
<tr>
<td>10.20.3.3</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.6/32</td>
<td>20</td>
<td>2/Int.</td>
<td>3</td>
<td>Dut-D</td>
</tr>
<tr>
<td>10.20.4.4</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.3.0/24</td>
<td>10</td>
<td>1/Int.</td>
<td>3</td>
<td>Dut-B</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.4.0/24</td>
<td>10</td>
<td>1/Int.</td>
<td>3</td>
<td>Dut-B</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.5.0/24</td>
<td>20</td>
<td>2/Int.</td>
<td>2</td>
<td>Dut-C</td>
</tr>
<tr>
<td>10.20.3.3</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.6.0/24</td>
<td>20</td>
<td>2/Int.</td>
<td>4</td>
<td>Dut-D</td>
</tr>
<tr>
<td>10.20.4.4</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.9.0/24</td>
<td>20</td>
<td>2/Int.</td>
<td>3</td>
<td>Dut-D</td>
</tr>
<tr>
<td>10.20.4.4</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.10.0/24</td>
<td>30</td>
<td>2/Int.</td>
<td>3</td>
<td>Dut-C</td>
</tr>
<tr>
<td>10.20.3.3</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flags: LFA = Loop-Free Alternate nexthop

---

*A:Dut-B#

*A:Dut-A# show router isis routes

### Route Table

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Metric</th>
<th>Lvl/Typ</th>
<th>Ver.</th>
<th>SysID/Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.1.0/24</td>
<td>10</td>
<td>1/Int.</td>
<td>5</td>
<td>Dut-A</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.3.0/24</td>
<td>20</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.4.0/24</td>
<td>20</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.5.0/24</td>
<td>30</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.9.0/24</td>
<td>60</td>
<td>1/Int.</td>
<td>52</td>
<td>Dut-F</td>
</tr>
<tr>
<td>10.10.21.6</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.10.0/24</td>
<td>70</td>
<td>1/Int.</td>
<td>52</td>
<td>Dut-F</td>
</tr>
<tr>
<td>10.10.21.6</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.12.0/24</td>
<td>20</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.13.0/24</td>
<td>10</td>
<td>1/Int.</td>
<td>7</td>
<td>Dut-A</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.14.0/24</td>
<td>20</td>
<td>1/Int.</td>
<td>52</td>
<td>Dut-F</td>
</tr>
<tr>
<td>Address</td>
<td>Metric</td>
<td>Type</td>
<td>Interface</td>
<td>Protocol</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------</td>
<td>--------</td>
<td>-----------</td>
<td>----------</td>
</tr>
<tr>
<td>10.10.21.6</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.15.0/24</td>
<td>30</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.16.0/24</td>
<td>30</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.21.0/24</td>
<td>10</td>
<td>1/Int.</td>
<td>48</td>
<td>Dut-A</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.1/32</td>
<td>0</td>
<td>1/Int.</td>
<td>10</td>
<td>Dut-A</td>
</tr>
<tr>
<td>20.20.1.2/32</td>
<td>10</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.3/32</td>
<td>20</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.4/32</td>
<td>20</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.5/32</td>
<td>30</td>
<td>1/Int.</td>
<td>137</td>
<td>Dut-B</td>
</tr>
<tr>
<td>10.10.1.2</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.6/32</td>
<td>10</td>
<td>1/Int.</td>
<td>52</td>
<td>Dut-F</td>
</tr>
<tr>
<td>10.10.21.6</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:100/120</td>
<td>10</td>
<td>1/Int.</td>
<td>5</td>
<td>Dut-A</td>
</tr>
<tr>
<td>::</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.1.0/24</td>
<td>10</td>
<td>1/Int.</td>
<td>65</td>
<td>Dut-A</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.10.13.0/24</td>
<td>10</td>
<td>1/Int.</td>
<td>65</td>
<td>Dut-A</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.0/24</td>
<td>10</td>
<td>1/Int.</td>
<td>65</td>
<td>Dut-A</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.20.1.1/32</td>
<td>0</td>
<td>1/Int.</td>
<td>65</td>
<td>Dut-A</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:100/120</td>
<td>10</td>
<td>1/Int.</td>
<td>65</td>
<td>Dut-A</td>
</tr>
<tr>
<td>::</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:300/120</td>
<td>20</td>
<td>1/Int.</td>
<td>116</td>
<td>Dut-B</td>
</tr>
<tr>
<td>FE80::2281:1FF:FE01:1-&quot;ip-3FFE::A0A:101&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:400/120</td>
<td>20</td>
<td>1/Int.</td>
<td>116</td>
<td>Dut-B</td>
</tr>
<tr>
<td>FE80::2281:1FF:FE01:1-&quot;ip-3FFE::A0A:101&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:500/120</td>
<td>30</td>
<td>1/Int.</td>
<td>130</td>
<td>Dut-B</td>
</tr>
<tr>
<td>FE80::2281:1FF:FE01:1-&quot;ip-3FFE::A0A:101&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:900/120</td>
<td>60</td>
<td>1/Int.</td>
<td>71</td>
<td>Dut-F</td>
</tr>
<tr>
<td>FE80::2285:FFFF:FE00:0-&quot;ies-1-3FFE::A0A:1501&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:A00/120</td>
<td>70</td>
<td>1/Int.</td>
<td>71</td>
<td>Dut-F</td>
</tr>
<tr>
<td>FE80::2289:FFFF:FE00:0-&quot;ies-1-3FFE::A0A:1501&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:C00/120</td>
<td>20</td>
<td>1/Int.</td>
<td>116</td>
<td>Dut-B</td>
</tr>
<tr>
<td>FE80::2281:1FF:FE01:1-&quot;ip-3FFE::A0A:101&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:D00/120</td>
<td>10</td>
<td>1/Int.</td>
<td>65</td>
<td>Dut-A</td>
</tr>
<tr>
<td>::</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:E00/120</td>
<td>20</td>
<td>1/Int.</td>
<td>71</td>
<td>Dut-F</td>
</tr>
<tr>
<td>FE80::2285:FFFF:FE00:0-&quot;ies-1-3FFE::A0A:1501&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:F00/120</td>
<td>30</td>
<td>1/Int.</td>
<td>130</td>
<td>Dut-B</td>
</tr>
<tr>
<td>FE80::2281:1FF:FE01:1-&quot;ip-3FFE::A0A:101&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:1000/120</td>
<td>30</td>
<td>1/Int.</td>
<td>130</td>
<td>Dut-B</td>
</tr>
<tr>
<td>FE80::2281:1FF:FE01:1-&quot;ip-3FFE::A0A:101&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:1500/120</td>
<td>10</td>
<td>1/Int.</td>
<td>65</td>
<td>Dut-A</td>
</tr>
<tr>
<td>::</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A0A:1600/120</td>
<td>30</td>
<td>1/Int.</td>
<td>127</td>
<td>Dut-B</td>
</tr>
<tr>
<td>FE80::2281:1FF:FE01:1-&quot;ip-3FFE::A0A:101&quot;</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3FFE::A14:101/128</td>
<td>0</td>
<td>1/Int.</td>
<td>65</td>
<td>Dut-A</td>
</tr>
<tr>
<td>::</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3FFE::A14:102/128                  10           1/Int.  116    Dut-B
   FE80::2281:1FF:FE01:1-"ip-3FFE::A0A:101" 2
3FFE::A14:103/128                  20           1/Int.  130    Dut-B
   FE80::2281:1FF:FE01:1-"ip-3FFE::A0A:101" 2
3FFE::A14:104/128                  20           1/Int.  127    Dut-B
   FE80::2281:1FF:FE01:1-"ip-3FFE::A0A:101" 2
3FFE::A14:105/128                  30           1/Int.  130    Dut-B
   FE80::2281:1FF:FE01:1-"ip-3FFE::A0A:101" 2
3FFE::A14:106/128                  10           1/Int.  71     Dut-F
   FE80::2285:FFFF:FE00:0-"ies-1-3FFE::A0A:1501" 2
-------------------------------------------------------------------------------
Routes : 43
*A:Dut-A#

*A:SRR# show router isis routes 1.1.1.0/24
-------------------------------------------------------------------------------
Route Table
-------------------------------------------------------------------------------
Prefix[Flags]                     Metric     Lvl/Typ    Ver.   SysID/Hostname
NextHop                          MT         AdminTag
-------------------------------------------------------------------------------
1.1.1.0/24 [L]                    7540       1/Int.     6109   SRL
   60.60.1.1                       0           0
-------------------------------------------------------------------------------
No. of Routes: 1
Flags: L = LFA nexthop available

*A:SRR# show router isis routes 1.1.1.0/24 alternative
-------------------------------------------------------------------------------
Route Table
-------------------------------------------------------------------------------
Prefix[Flags]                     Metric     Lvl/Typ    Ver.   SysID/Hostname
NextHop                          MT         AdminTag
Alt=Nexthop                       Alt-Metric Alt-Type
-------------------------------------------------------------------------------
1.1.1.0/24
   60.60.1.1                       7550       1/Int.     6114   SRL
   11.22.12.4 (LFA)                16784764    linkProtection
-------------------------------------------------------------------------------
No. of Routes: 1
Flags: LFA = Loop-Free Alternate nexthop

*A:SRR#

*A:SRR# show router isis routes 1.1.1.0/24
-------------------------------------------------------------------------------
Route Table
-------------------------------------------------------------------------------
Prefix[Flags]                     Metric     Lvl/Typ    Ver.   SysID/Hostname
NextHop                          MT         AdminTag
-------------------------------------------------------------------------------
1.1.1.0/24 [L]                    7540       1/Int.     6109   SRL
   60.60.1.1                       0           0
-------------------------------------------------------------------------------
No. of Routes: 1
Flags: L = LFA nexthop available

*A:SRR# show router isis routes 1.1.1.0/24 alternative
Route Table

Prefix Flags Metric Lvl/Typ Ver. SysID/Hostname NextHop MT AdminTag Alt-Nexthop Alt-Metric Alt-Type

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Flags</th>
<th>Metric</th>
<th>Lvl/Typ</th>
<th>Ver.</th>
<th>SysID/Hostname</th>
<th>NextHop</th>
<th>MT</th>
<th>AdminTag</th>
<th>Alt-Nexthop</th>
<th>Alt-Metric</th>
<th>Alt-Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.0/24</td>
<td></td>
<td>7550</td>
<td>1/Int.</td>
<td>6114</td>
<td>SRL</td>
<td>60.60.1.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60.60.1.1</td>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11.22.12.4 (LFA)</td>
<td></td>
<td>16784764</td>
<td>linkProtection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

No. of Routes: 1
Flags: LFA = Loop-Free Alternate nexthop

*A:SRR#

spf

Syntax  spf [detail] [lfa]

Context  show>router>isis

Description  This command displays information regarding SPF calculation.

Output  Router ISIS Output — The following table describes the output fields for ISIS SPF.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>The route node and mask.</td>
</tr>
<tr>
<td>Interface</td>
<td>The outgoing interface name for the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>The route’s metric.</td>
</tr>
<tr>
<td>Nexthop</td>
<td>The system ID of nexthop or hostname.</td>
</tr>
<tr>
<td>SNPA</td>
<td>The Subnetwork Points of Attachment (SNPA) where a router is physically attached to a subnetwork.</td>
</tr>
</tbody>
</table>

Sample Output

linus-212>show>router>isis# show router isis spf

Path Table

<table>
<thead>
<tr>
<th>Node Interface Nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>linus-211.00 ab linus-211</td>
</tr>
<tr>
<td>x linux-222 *</td>
</tr>
<tr>
<td>linus-216.00 ab linus-211</td>
</tr>
<tr>
<td>linus-216.00 ab linus-211</td>
</tr>
<tr>
<td>linus-216.01 ab linus-211</td>
</tr>
</tbody>
</table>

7450 ESS OS Routing Protocols Guide  Page 521
A:ALA-A# show router isis spf

Path Table

<table>
<thead>
<tr>
<th>Node</th>
<th>Interface</th>
<th>Nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>abr_sjc.00</td>
<td>if2/2</td>
<td>dist_oak</td>
</tr>
<tr>
<td>abr_sjc.00</td>
<td>if2/3</td>
<td>dist_nj</td>
</tr>
<tr>
<td>dist_oak.00</td>
<td>if2/2</td>
<td>dist_oak</td>
</tr>
<tr>
<td>dist_nj.00</td>
<td>if2/3</td>
<td>dist_nj</td>
</tr>
<tr>
<td>acc_nj.00</td>
<td>if2/3</td>
<td>dist_nj</td>
</tr>
<tr>
<td>acc_ri.00</td>
<td>if2/3</td>
<td>dist_nj</td>
</tr>
<tr>
<td>core_west.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>core_east.00</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>asbr_west.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>asbr_east.00</td>
<td>if2/5</td>
<td>asbr_east</td>
</tr>
<tr>
<td>abr_sjc.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>abr_sjc.00</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>abr_lax.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>abr_lax.00</td>
<td>if2/5</td>
<td>asbr_east</td>
</tr>
<tr>
<td>abr_dfw.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>abr_dfw.00</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>dist_arl.00</td>
<td>if2/5</td>
<td>asbr_east</td>
</tr>
<tr>
<td>dist_arl.00</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>dist_arl.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>dist_msq.00</td>
<td>if2/5</td>
<td>asbr_east</td>
</tr>
<tr>
<td>dist_msq.00</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>dist_msq.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>acc_arl.00</td>
<td>if2/5</td>
<td>asbr_east</td>
</tr>
<tr>
<td>acc_arl.00</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>acc_arl.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>acc_msq.00</td>
<td>if2/5</td>
<td>asbr_east</td>
</tr>
<tr>
<td>acc_msq.00</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>acc_msq.00</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>acc_msq.03</td>
<td>if2/5</td>
<td>asbr_east</td>
</tr>
<tr>
<td>acc_msq.03</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>acc_msq.03</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
<tr>
<td>acc_msq.04</td>
<td>if2/5</td>
<td>asbr_east</td>
</tr>
<tr>
<td>acc_msq.04</td>
<td>lag-1</td>
<td>core_east</td>
</tr>
<tr>
<td>acc_msq.04</td>
<td>if2/8</td>
<td>core_west</td>
</tr>
</tbody>
</table>

A:ALA-A# show router isis spf detail

Path Table

<table>
<thead>
<tr>
<th>Node</th>
<th>Interface</th>
<th>Metric</th>
<th>SNPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>abr_sjc.00</td>
<td>if2/2</td>
<td>20</td>
<td>00:00:00:00:00:00</td>
</tr>
<tr>
<td>abr_sjc.00</td>
<td>if2/3</td>
<td>00</td>
<td>00:00:00:00:00:00</td>
</tr>
</tbody>
</table>

A:ALA-A#
Node : dist_oak.00 Metric : 10
Interface : if2/2 SNPA : 00:00:00:00:00:00
Nexthop : dist_oak

Node : dist_nj.00 Metric : 10
Interface : if2/3 SNPA : 00:00:00:00:00:00
Nexthop : dist_nj

Node : acc_nj.00 Metric : 20
Interface : if2/3 SNPA : 00:00:00:00:00:00
Nexthop : dist_nj

Node : acc_ri.00 Metric : 20
Interface : if2/3 SNPA : 00:00:00:00:00:00
Nexthop : dist_nj

Node : core_west.00 Metric : 10
Interface : if2/8 SNPA : 00:00:00:00:00:00
Nexthop : core_west

...
<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>SNPA</th>
<th>Nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESS-7.0B</td>
<td>16778214</td>
<td>sru4-3</td>
<td>n/a</td>
<td>SRU4</td>
</tr>
<tr>
<td>SRC.00</td>
<td>1000</td>
<td>src-asap-2</td>
<td>n/a</td>
<td>SRC</td>
</tr>
<tr>
<td>SRC.01</td>
<td>2000</td>
<td>aps-10</td>
<td>n/a</td>
<td>SRC</td>
</tr>
<tr>
<td>SRC.02</td>
<td>16778214</td>
<td>src-asap-2</td>
<td>n/a</td>
<td>SRC</td>
</tr>
<tr>
<td>SRC.03</td>
<td>1063</td>
<td>aps-10</td>
<td>n/a</td>
<td>SRC</td>
</tr>
<tr>
<td>SRL.00</td>
<td>1000</td>
<td>aps-1</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.00</td>
<td>1000</td>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.00</td>
<td>1000</td>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.09</td>
<td>2000</td>
<td>aps-1</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.09</td>
<td>2000</td>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.0A</td>
<td>2000</td>
<td>aps-1</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.0A</td>
<td>2000</td>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.0A</td>
<td>2000</td>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.00</td>
<td>2000</td>
<td></td>
<td></td>
<td>SRL</td>
</tr>
</tbody>
</table>

**Level 2**

<table>
<thead>
<tr>
<th>Node</th>
<th>Metric</th>
<th>Interface</th>
<th>SNPA</th>
<th>Nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>SRL.00</td>
<td>1000</td>
<td>aps-1</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.00</td>
<td>1000</td>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.00</td>
<td>1000</td>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.09</td>
<td>2000</td>
<td>aps-1</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.09</td>
<td>2000</td>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.09</td>
<td>2000</td>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.0A</td>
<td>2000</td>
<td>aps-1</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.0A</td>
<td>2000</td>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRL.0A</td>
<td>2000</td>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
</tr>
<tr>
<td>SRU4.00</td>
<td>2000</td>
<td></td>
<td></td>
<td>SRU4</td>
</tr>
<tr>
<td>Interface</td>
<td>SNPA</td>
<td>Nexthop</td>
<td>Node</td>
<td>Metric</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>----------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>aps-1</td>
<td>n/a</td>
<td>SRL</td>
<td>SRU4.00</td>
<td>2000</td>
</tr>
<tr>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>germ-1</td>
<td>16778214</td>
</tr>
<tr>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.00</td>
<td>16778214</td>
</tr>
<tr>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.05</td>
<td>16778214</td>
</tr>
<tr>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.06</td>
<td>16778214</td>
</tr>
<tr>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.06</td>
<td>16778214</td>
</tr>
<tr>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.06</td>
<td>16778214</td>
</tr>
<tr>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.06</td>
<td>16778214</td>
</tr>
<tr>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.06</td>
<td>16778214</td>
</tr>
<tr>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.06</td>
<td>16778214</td>
</tr>
<tr>
<td>if-30.30.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.06</td>
<td>16778214</td>
</tr>
<tr>
<td>if-40.40.1.2</td>
<td>n/a</td>
<td>SRL</td>
<td>ESS-7.06</td>
<td>16778214</td>
</tr>
</tbody>
</table>
Interface : ess-7-1                  SNPA     : 00:16:4d:c1:25:e4
Nexthop   : ESS-7

Node     : ESS-7.0E                Metric   : 16778214
Interface : ess-7-1                SNPA     : 00:16:4d:c1:25:e4
Nexthop   : ESS-7

Node     : ESS-7.12                Metric   : 16778214
Interface : ess-7-1                SNPA     : 00:16:4d:c1:25:e4
Nexthop   : ESS-7

Node     : ESS-7.12                Metric   : 16778214
Interface : germ-1                  SNPA     : n/a
Nexthop   : SROne

Node     : SRC.00                   Metric   : 1000
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

LFA intf : aps-1                   LFA Metric : 2063
LFA nh   : SRL                      LFA type   : linkProtection

Node     : SRC.05                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.06                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.07                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.08                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.09                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.0A                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.0B                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.0C                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.0D                   Metric   : 16778214
Interface : src-asap-1              SNPA     : n/a
Nexthop   : SRC

Node     : SRC.0E                   Metric   : 16778214
Interface : src-asap-1 SNPA : n/a
Nexthop : SRC

Node : SROne.00 Metric : 1000
Interface : germ-1 SNPA : n/a
Nexthop : SROne

LFA intf : aps-1 LFA Metric : 2000
LFA nh : SRL LFA type : linkProtection

*A:SRR>config>router>isis#

spf-log

Syntax spf-log [detail]

Context show>router>isis

Description Displays the IS-IS SPF log information.

Parameters detail — Displays detailed logged information.

Output Router ISIS SFP Log Output — The following table describes the ISIS SPF log output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>When</td>
<td>Displays the timestamp when the SPF run started on the system</td>
</tr>
<tr>
<td>Duration</td>
<td>Displays the time (in hundredths of a second) required to complete the SPF run.</td>
</tr>
<tr>
<td>L1 Nodes</td>
<td>Displays the number of level 1 nodes involved in the SPF run.</td>
</tr>
<tr>
<td>L2 Nodes</td>
<td>Displays the number of level 2 nodes involved in the SPF run.</td>
</tr>
<tr>
<td>Event Count</td>
<td>Displays the number of SPF events that triggered the SPF calculation.</td>
</tr>
<tr>
<td>Log Entries</td>
<td>The total number of log entries.</td>
</tr>
</tbody>
</table>

Sample Output

*A:Dut-A# show router isis spf-log

<table>
<thead>
<tr>
<th>When</th>
<th>Duration</th>
<th>L1 Nodes</th>
<th>L2 Nodes</th>
<th>Event Count</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/20/2012 08:57:33</td>
<td>&lt;0.01s</td>
<td>6</td>
<td>6</td>
<td>141</td>
<td>Reg</td>
</tr>
<tr>
<td>02/20/2012 08:57:34</td>
<td>&lt;0.01s</td>
<td>14</td>
<td>14</td>
<td>20</td>
<td>Reg</td>
</tr>
<tr>
<td>02/20/2012 08:57:34</td>
<td>&lt;0.01s</td>
<td>28</td>
<td>28</td>
<td>20</td>
<td>Lfa</td>
</tr>
<tr>
<td>02/20/2012 08:57:36</td>
<td>&lt;0.01s</td>
<td>14</td>
<td>14</td>
<td>18</td>
<td>Reg</td>
</tr>
<tr>
<td>02/20/2012 08:57:36</td>
<td>&lt;0.01s</td>
<td>28</td>
<td>28</td>
<td>18</td>
<td>Lfa</td>
</tr>
<tr>
<td>02/20/2012 08:57:44</td>
<td>&lt;0.01s</td>
<td>14</td>
<td>14</td>
<td>3</td>
<td>Reg</td>
</tr>
</tbody>
</table>
A:SetupCLI# show router isis spf-log detail

ISIS SPF Log

When : 10/01/2011 03:40:25              Duration : <0.01s
L1 Nodes : 1                             L2 Nodes : 1
Trigger LSP: SetupCLI.00-00              Event Count : 78
SPF Type : Reg                           Reason : LSPCONTENT

When : 10/01/2011 03:40:26              Duration : <0.01s
L1 Nodes : 1                             L2 Nodes : 1
Trigger LSP: SetupCLI.00-00              Event Count : 1
SPF Type : Reg                           Reason : LSPCONTENT

When : 10/01/2011 03:40:25              Duration : <0.01s
L1 Nodes : 1                             L2 Nodes : 1
Trigger LSP: SetupCLI.00-00              Event Count : 25
SPF Type : Reg                           Reason : NEWAREA NEWREACH LSPCONTENT MANUALREQ

When : 10/01/2011 03:40:27              Duration : <0.01s
L1 Nodes : 1                             L2 Nodes : 1
Trigger LSP: SetupCLI.00-00              Event Count : 1
SPF Type : Reg                           Reason : LSPCONTENT

When : 10/01/2011 03:40:27              Duration : <0.01s
L1 Nodes : 0                             L2 Nodes : 0
Trigger LSP: SetupCLI.00-00              Event Count : 1
SPF Type : Lfa                           Reason : LSPCONTENT

When : 10/01/2011 03:40:25              Duration : <0.01s
L1 Nodes : 1                             L2 Nodes : 1
Trigger LSP: SetupCLI.00-00              Event Count : 75
SPF Type : Reg                           Reason : LSPCONTENT

When : 10/01/2011 03:40:27              Duration : <0.01s
L1 Nodes : 1                             L2 Nodes : 1
Trigger LSP: SetupCLI.00-00              Event Count : 1
SPF Type : Reg                           Reason : LSPCONTENT

A:SetupCLI#

A:ALA-48# show router isis spf-log

ISIS SPF Log
When                      Duration       L1 Nodes   L2 Nodes   Event Count
-------------------------------------------------------------------------------
01/30/2007 11:01:54       <0.01s         1          1          3
-------------------------------------------------------------------------------
Log Entries : 1
===============================================================================

Statistics

Syntax       statistics

Context      show>router>isis

Description  This command displays information regarding IS-IS traffic statistics.

Output       IS-IS Statistics Output — This table describes IS-IS statistics output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge Initiated</td>
<td>The number of times purges have been initiated.</td>
</tr>
<tr>
<td>SPF Runs</td>
<td>The number of times shortest path first calculations have been made.</td>
</tr>
<tr>
<td>LSP Regens</td>
<td>The count of LSP regenerations.</td>
</tr>
<tr>
<td>Requests</td>
<td>The number of CSPF requests made to the protocol.</td>
</tr>
<tr>
<td>Paths Found</td>
<td>The number of responses to CSPF requests for which paths satisfying the</td>
</tr>
<tr>
<td></td>
<td>constraints were found.</td>
</tr>
<tr>
<td>PDU Type</td>
<td>The PDU type.</td>
</tr>
<tr>
<td>Received</td>
<td>The count of link state PDUs received by this instance of the protocol.</td>
</tr>
<tr>
<td>Processed</td>
<td>The count of link state PDUs processed by this instance of the protocol.</td>
</tr>
<tr>
<td>Dropped</td>
<td>The count of link state PDUs dropped by this instance of the protocol.</td>
</tr>
<tr>
<td>Sent</td>
<td>The count of link state PDUs sent out by this instance of the protocol.</td>
</tr>
<tr>
<td>Retransmitted</td>
<td>The count of link state PDUs that had to be retransmitted by this</td>
</tr>
<tr>
<td></td>
<td>instance of the protocol.</td>
</tr>
</tbody>
</table>

Sample Output

*A:SRR>config>router>isis# show router isis statistics

7450 ESS OS Routing Protocols Guide
Show Commands

===============================================================================
ISIS Statistics
===============================================================================
ISIS Instance : 0                       SPF Runs     : 6274
Purge Initiated : 2654                    LSP Regens. : 250706

CSPF Statistics
Requests        : 4991                    Request Drops : 0
Paths Found      : 20                      Paths Not Found: 4971

LFA Statistics
LFA Runs        : 6274
-------------------------------------------------------------------------------

PDU Type   Received   Processed  Dropped    Sent       Retransmitted
-------------------------------------------------------------------------------
LSP        9997718    9997718    0          7060383    0
IIH        149110     149110     0          171964     0
CSNP       411712     411712     0          204861     0
PSNP       528654     528654     0          615952     0
Unknown    0          0          0          0          0
-------------------------------------------------------------------------------

*A:SRR>config>router>isis#

status

Syntax      status
Context     show>router>isis
Description This command displays information regarding IS-IS status.

Output      IS-IS Status Output — The following table describes IS-IS status output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System-id</td>
<td>Neighbor system ID.</td>
</tr>
</tbody>
</table>
| Admin State       | Up — IS-IS is administratively up.
|                   | Down — IS-IS is administratively down. |
| Ipv4 Routing      | Enabled — IPv4 routing is enabled. |
|                   | Disabled — IPv4 routing is disabled. |
| Last Enabled      | The date/time when IS-IS was last enabled in the router. |
| Level Capability  | The routing level for the IS-IS routing process. |
| Authentication Check | True — All IS-IS mismatched protocol packets are rejected. |
Sample Output

```
A:setupcli# show router isis status
-----------------------------------------------------------------------------------
ISIS Status
-----------------------------------------------------------------------------------
System Id            : 0100.2003.0040
Admin State          : Up
Ipv4 Routing         : Enabled
Ipv6 Routing         : Disabled
Last Enabled         : 10/01/2011 04:11:47
Level Capability     : L1L2
Authentication Check : True
Authentication Type  : MD5
CSNP-Authentication  : Enabled
HELLO-Authentication : Enabled
PSNP-Authentication  : Enabled
Traffic Engineering  : Enabled
GR Helper Mode       : Enabled
LSP Lifetime         : 2400
LSP Wait             : 120 sec (Max)   0 sec (Initial)   1 sec (Second)
LSP MTU Size         : 9190  (Config)  9190  (Oper)
Adjacency Check      : strict
L1 Auth Type         : password
L2 Auth Type         : md5
L1 CSNP-Authentication*: Enabled
L1 HELLO-Authentication*: Enabled
L1 PSNP-Authentication*: Enabled
L1 Preference        : 30
L2 Preference        : 22
L1 Ext. Preference   : 40
L2 Ext. Preference   : 34
```

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Type</td>
<td>The method of authentication used to verify the authenticity of packets sent by neighboring routers on an IS-IS interface.</td>
</tr>
<tr>
<td>Traffic Engineering</td>
<td>Enabled — TE is enabled for the router.</td>
</tr>
<tr>
<td></td>
<td>Disabled — TE is disabled so that TE metrics are not generated and are ignored when received by this node.</td>
</tr>
<tr>
<td>Graceful Restart</td>
<td>Enabled — Graceful restart is enabled for this instance of IS-IS on the router.</td>
</tr>
<tr>
<td></td>
<td>Disabled — Graceful restart capability is disabled for this instance of IS-IS on the router.</td>
</tr>
<tr>
<td>Ldp Sync Admin State</td>
<td>Indicates whether the IGP-LDP synchronization feature is enabled or disabled on all interfaces participating in the OSPF routing protocol.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>L1 Wide Metrics</td>
<td>Enabled</td>
</tr>
<tr>
<td>L2 Wide Metrics</td>
<td>Enabled</td>
</tr>
<tr>
<td>L1 LSDB Overload</td>
<td>Disabled</td>
</tr>
<tr>
<td>L2 LSDB Overload</td>
<td>Disabled</td>
</tr>
<tr>
<td>L1 LSPs</td>
<td>1</td>
</tr>
<tr>
<td>L2 LSPs</td>
<td>1</td>
</tr>
<tr>
<td>L1 Default Metric</td>
<td>10</td>
</tr>
<tr>
<td>L2 Default Metric</td>
<td>10</td>
</tr>
<tr>
<td>L1 IPv6 Def Metric</td>
<td>10</td>
</tr>
<tr>
<td>L2 IPv6 Def Metric</td>
<td>10</td>
</tr>
<tr>
<td>Last SPF</td>
<td>10/01/2011 04:11:49</td>
</tr>
<tr>
<td>SPF Wait</td>
<td>120 sec (Max) 1000 ms (Initial) 1000 ms (Second)</td>
</tr>
<tr>
<td>Export Policies</td>
<td>None</td>
</tr>
<tr>
<td>Multicast Import</td>
<td>None</td>
</tr>
<tr>
<td>Multi-topology</td>
<td>Disabled</td>
</tr>
<tr>
<td>Advertise-Passive-On*</td>
<td>Enabled</td>
</tr>
<tr>
<td>Suppress Default</td>
<td>Enabled</td>
</tr>
<tr>
<td>Default Route Tag</td>
<td>1</td>
</tr>
<tr>
<td>Area Addresses</td>
<td>49.0001</td>
</tr>
<tr>
<td></td>
<td>47.1234.1234.1234.1234.ffff</td>
</tr>
<tr>
<td>Ldp Sync Admin State</td>
<td>Down</td>
</tr>
<tr>
<td>LDP-over-RSVP</td>
<td>Enabled</td>
</tr>
<tr>
<td>RSVP-Shortcut</td>
<td>Enabled</td>
</tr>
<tr>
<td>Advertise-Tunnel-Link</td>
<td>Disabled</td>
</tr>
<tr>
<td>Export Limit</td>
<td>0</td>
</tr>
<tr>
<td>Exp Lmt Log Percent</td>
<td>0</td>
</tr>
<tr>
<td>Total Exp Routes(L1)</td>
<td>0</td>
</tr>
<tr>
<td>Total Exp Routes(L2)</td>
<td>0</td>
</tr>
<tr>
<td>IID TLV</td>
<td>Enabled</td>
</tr>
<tr>
<td>All-L1-MacAddr</td>
<td>01:80:c2:00:00:14</td>
</tr>
<tr>
<td>All-L2-MacAddr</td>
<td>01:80:c2:00:00:15</td>
</tr>
<tr>
<td>Loopfree-Alternate</td>
<td>Enabled</td>
</tr>
<tr>
<td>L1 LFA</td>
<td>Included</td>
</tr>
<tr>
<td>L2 LFA</td>
<td>Included</td>
</tr>
</tbody>
</table>

* indicates that the corresponding row element may have been truncated.

Task 113366: IPFRR

*SRR#config>router>isis# show router isis status

ISIS Status

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Id</td>
<td>1100.2000.1002</td>
</tr>
<tr>
<td>Admin State</td>
<td>Up</td>
</tr>
<tr>
<td>Ipv4 Routing</td>
<td>Enabled</td>
</tr>
<tr>
<td>Ipv6 Routing</td>
<td>Enabled, Native</td>
</tr>
<tr>
<td>Last Enabled</td>
<td>07/25/2011 18:11:34</td>
</tr>
<tr>
<td>Level Capability</td>
<td>L1L2</td>
</tr>
<tr>
<td>Authentication Check</td>
<td>True</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>None</td>
</tr>
<tr>
<td>CSNP-Authentication</td>
<td>Enabled</td>
</tr>
<tr>
<td>HELLO-Authentication</td>
<td>Enabled</td>
</tr>
<tr>
<td>PSNP-Authentication</td>
<td>Enabled</td>
</tr>
<tr>
<td>Traffic Engineering</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Graceful Restart : Disabled
GR Helper Mode : Disabled
LSP Lifetime : 350
LSP Wait : 5 sec (Max) 0 sec (Initial) 1 sec (Second)
LSP MTU Size : 1492 (Config) 1492 (Oper)
Adjacency Check : loose
L1 Auth Type : none
L2 Auth Type : none
L1 CSNP-Authentication*: Enabled
L1 HELLO-Authentication*: Enabled
L1 PSNP-Authentication*: Enabled
L1 Preference : 15
L2 Preference : 18
L1 Ext. Preference : 160
L2 Ext. Preference : 165
L1 Wide Metrics : Enabled
L2 Wide Metrics : Enabled
L1 LSDB Overload : Disabled
L2 LSDB Overload : Disabled
L1 LSPs : 86
L2 LSPs : 113
L1 Default Metric : 10
L2 Default Metric : 10
L1 IPv6 Def Metric : 10
L2 IPv6 Def Metric : 10
Last SPF : 07/26/2011 15:27:09
SPF Wait : 10 sec (Max) 1000 ms (Initial) 1000 ms (Second)
Export Policies : isis_from_ALL_to_0
Multicast Import : both
Multi-topology : Enabled
Advertise-Passive-On*: Disabled
Suppress Default : Disabled
Default Route Tag : None
Area Addresses : 49.0001
Ldp Sync Admin State : Up
LDP-over-RSVP : Enabled
RSVP-Shortcut : Disabled
Advertise-Tunnel-Link: Disabled
Export Limit : 0
Exp Lmt Log Percent : 0
Total Exp Routes(L1) : 0
Total Exp Routes(L2) : 0
IID TLV : Disabled
All-L1-MacAddr : 01:80:c2:00:00:14
All-L2-MacAddr : 01:80:c2:00:00:15
Loopfree-Alternate : Enabled

* indicates that the corresponding row element may have been truncated.
*A:SRR>config>router>isis#
Show Commands

summary-address

**Syntax**

```
summary-address [ip-address [mask]]
```

**Context**

```
show>router>isis
```

**Description**

Displays ISIS summary addresses.

**Output**

**Router ISIS Summary Address Output** — The following table describes the ISIS summary address output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>The IP address.</td>
</tr>
<tr>
<td>Level</td>
<td>Specifies the IS-IS level from which the prefix should be summarized.</td>
</tr>
</tbody>
</table>

**Sample Output**

```
A:ALA-48# show router isis summary-address
===============================================================================
ISIS Summary Address
===============================================================================
<table>
<thead>
<tr>
<th>Address</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0.0/8</td>
<td>L1</td>
</tr>
<tr>
<td>2.1.0.0/24</td>
<td>L1L2</td>
</tr>
<tr>
<td>3.1.2.3/32</td>
<td>L2</td>
</tr>
</tbody>
</table>
===============================================================================
Summary Addresses : 3
A:ALA-48#
```

topology

**Syntax**

```
topology [ipv4-unicast | mt mt-id-number] [detail]
```

**Context**

```
show>router>isis
```

**Description**

This command shows IS-IS topology information.

**Parameters**

- **ipv4-unicast** — Displays IPv4 unicast parameters.
- **mt mt-id-number** — Displays multi-topology parameters.
  - **Values**
    - 0, 2
- **detail** — Displays detailed topology information.

**Output**

**Router ISIS Topology Output** — The following table describes the ISIS topology output fields.
Sample Output

*A:Dut-A# show router isis topology

Topology Table

<table>
<thead>
<tr>
<th>Node</th>
<th>Interface</th>
<th>Nexthop</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-IS IP paths (MT-ID 0), Level 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dut-B.00</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-B.01</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-CA.00</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-CA.01</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-CA.02</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-CA.05</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-DA.00</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-DA.01</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-E.00</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-F.00</td>
<td>ies-1-3FFE::A0A:1501</td>
<td>Dut-F</td>
</tr>
<tr>
<td>Dut-F.01</td>
<td>ies-1-3FFE::A0A:1501</td>
<td>Dut-F</td>
</tr>
<tr>
<td>Dut-F.02</td>
<td>ies-1-3FFE::A0A:1501</td>
<td>Dut-F</td>
</tr>
<tr>
<td>IS-IS IP paths (MT-ID 0), Level 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dut-B.00</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-B.01</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-CA.00</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-CA.01</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-CA.02</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-CA.05</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-DA.00</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-DA.01</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-E.00</td>
<td>ip-3FFE::A0A:101</td>
<td>Dut-B</td>
</tr>
<tr>
<td>Dut-F.00</td>
<td>ies-1-3FFE::A0A:1501</td>
<td>Dut-F</td>
</tr>
<tr>
<td>Dut-F.01</td>
<td>ies-1-3FFE::A0A:1501</td>
<td>Dut-F</td>
</tr>
<tr>
<td>Dut-F.02</td>
<td>ies-1-3FFE::A0A:1501</td>
<td>Dut-F</td>
</tr>
</tbody>
</table>

*A:Dut-A#
Clear Commands

**isis**

**Syntax**
\[ isis [isis-instance] \]

**Context**
clear>router>isis

**Description**
This command enables the context to clear and reset ISIS protocol entities.

**Parameters**
- **isis-instance** — Specifies the IS-IS instance.
- **Values**
  
  1 — 31

**adjacency**

**Syntax**
\[ adjacency [system-id] \]

**Context**
clear>router>isis

**Description**
This command clears and resets the entries from the IS-IS adjacency database.

**Parameters**
- **system-id** — When the system ID is entered, only the specified entries are removed from the IS-IS adjacency database.

**database**

**Syntax**
\[ database [system-id] \]

**Context**
clear>router>isis

**Description**
This command removes the entries from the IS-IS link-state database which contains information about PDUs.

**Parameters**
- **system-id** — When the system ID is entered, only the specified entries are removed from the IS-IS link-state database.
export

Syntax    export
Context   clear>router>isis
Description This command re-evaluates route policies participating in the export mechanism, either as importers or exporters of routes.

spf-log

Syntax    spf-log
Context   clear>router>isis
Description This command clears the SPF log.

statistics

Syntax    statistics
Context   clear>router>isis
Description This command clears and resets IS-IS statistics.
Debug Commands

adjacency

Syntax  [no] adjacency [ip-int-name | ip-address | nbr-system-id]
Context debug>router>isis
Description This command enables debugging for IS-IS adjacency. The no form of the command disables debugging.

cspf

Syntax  [no] cspf
Context debug>router>isis
Description This command enables debugging for IS-IS cspf. The no form of the command disables debugging.

graceful-restart

Syntax  [no] graceful-restart
Context debug>router>isis
Description This command enables debugging for IS-IS graceful-restart. The no form of the command disables debugging.

interface

Syntax  interface [ip-int-name | ip-address]
no interface
Context debug>router>isis
Description This command enables debugging for IS-IS interface. The no form of the command disables debugging.
leak

Syntax     leak [ip-address]
           no leak

Context     debug>router>isis

Description  This command enables debugging for IS-IS leaks.
              The no form of the command disables debugging.

lsdb

Syntax     [no] lsdb [level-number] [system-id | lsp-id]

Context     debug>router>isis

Description  This command enables debugging for Link State DataBase (LSDB).
              The no form of the command disables debugging.

misc

Syntax     [no] misc

Context     debug>router>isis

Description  This command enables debugging for IS-IS misc.
              The no form of the command disables debugging.

packet

Syntax     packet [packet-type] [ip-int-name | ip-address] [detail]

Context     debug>router>isis

Description  This command enables debugging for IS-IS packets.
              The no form of the command disables debugging.
Debug Commands

rtm

Syntax  

rtm [ip-address]  
no rtm  

Context  
debug>router>isis  

Description  
This command enables debugging for IS-IS route table manager (RTM). The no form of the command disables debugging.

spf

Syntax  

[no] spf [level-number] [system-id]  

Context  
debug>router>isis  

Description  
This command enables debugging for IS-IS SPF. The no form of the command disables debugging.
In This Chapter

This chapter provides information to configure BGP.

Topics in this chapter include:

- BGP Overview on page 542
  - BGP Communication on page 542
  - Group Configuration and Peers on page 544
  - Hierarchical Levels on page 545
  - Route Reflection on page 545
  - BGP Route Tunnel on page 549
  - RSVP-TE LSP Shortcut for BGP Next-Hop Resolution on page 551
  - BGP Confederations on page 553
  - Command Interactions and Dependencies on page 567
    - Changing the Autonomous System Number on page 567
    - Changing the Router ID at the Configuration Level on page 568
    - Changing the Local AS Number on page 568
    - Hold Time and Keep Alive Timer Dependencies on page 569
    - Import and Export Route Policies on page 570
    - Route Damping and Route Policies on page 570
    - AS Override on page 570
    - TTL Security for LDP on page 575
- BGP Configuration Process Overview on page 576
- Configuration Notes on page 577
BGP Overview

Border Gateway Protocol (BGP) is an inter-autonomous system routing protocol. An autonomous system is a network or a group of routers logically organized and controlled by a common network administration. BGP enables routers to exchange network reachability information, including information about other ASs that traffic must traverse to reach other routers in other ASs. In order to implement BGP in the base router instance, the AS number must be specified in the config-router context. A routerBGP configuration must contain at least one group and include information about at least one neighbor (peer).

AS paths are the routes to each destination. Other attributes, such as the path’s origin, the multiple exit discriminator (MED), the local preference and communities included with the route are called path attributes. When BGP interprets routing and topology information, loops can be detected and eliminated. Route preference for routes learned from the configured peer(s) can be enabled among groups of routes to enforce administrative preferences and routing policy decisions.

BGP Communication

There are three types of BGP peers, internal BGP (IBGP), confederation external BGP (confed-EBGP), and external BGP (EBGP) (Figure 19).

- IBGP is used to communicate with peers in the same autonomous system. Routes received from an IBGP peer in the same autonomous system are not advertised to other IBGP peers (unless the router is a route reflector) but can be advertised to an EBGP peer.
- Confed-EBGP is used to communicate with peers in a different member-AS of the same BGP confederation. More details are provided in the section on BGP confederations.
- EBGP is used to communicate with peers in different autonomous systems. Routes received from an EBGP peer in a different AS can be advertised to both EBGP and IBGP peers.

Autonomous systems share routing information, such as routes to each destination and information about the route or AS path, with other ASs using BGP. Routing tables contain lists of known routers, reachable addresses, and associated path cost metrics to each router. BGP uses the information and path attributes to compile a network topology.

Message Types

Four message types are used by BGP to negotiate parameters, exchange routing information and indicate errors. They are:

- Open Message — After a transport protocol connection is established, the first message sent by each side is an Open message. If the Open message is acceptable, a Keepalive
message confirming the Open is sent back. Once the Open is confirmed, Update, Keepalive, and Notification messages can be exchanged.

Open messages consist of the BGP header and the following fields:

→ **Version** — The current BGP version number is 4.

→ **Local AS number** — For the base router BGP instance, this is usually the autonomous system number configured in the `config>router` context, however, it can be overridden on a per-session basis using the `local-as` command.

→ **Hold time** — The proposed maximum time BGP will wait between successive messages (either keep alive or update) from its peer, before closing the connection. The actual hold time is the minimum of the configured hold-time for the session and the hold-time in the peer's Open message. If this minimum is below a configured threshold (min hold time), the connection attempt is rejected.

→ **BGP identifier** — The router ID of the BGP speaker. In Open messages sent by 7x50, the BGP identifier comes from the `router-id` configured under `config>router`; if that is not configured then the `router-id` configured under `config>router` is used; if that too is not configured then the system interface IP address is used as the router ID. Note that a change of the router ID in the `config>router>bgp` context causes all BGP sessions to be reset immediately while other changes resulting in a new BGP identifier only take effect after BGP is shutdown and re-enabled.

→ **Update Message** — Update messages are used to transfer routing information between BGP peers. The information contained in the message can be used to construct a graph describing the relationships of the various autonomous systems. By applying rules, routing information loops and some other anomalies can be detected and removed from the inter-AS routing.

The update messages consist of a BGP header and the following fields:

→ **Unfeasible routes length** — The length of the withdrawn routed field, which lists the routes being withdrawn from service because they are considered unreachable.

→ **Withdrawn routes** — The associated IP address prefixes for the routes withdrawn from service.

→ **Total path attribute length** — The total length of the path attributes field that provides the attributes for a possible route to a destination.

→ **Path attributes** — The path attributes presented in variable length TLV format.

→ **Network layer reachability information (NLRI)** — IPv4 address prefixes of that are advertised as being reachable over the associated path.

→ **Keepalive Message** — Keepalive messages, consisting of only a 19 octet message header, are exchanged between peers frequently so hold timers do not expire. The keepalive messages are one method of determining a connectivity failure to the peer.

→ **Notification** — A Notification message is sent when an error condition is detected. The peering session is terminated and the BGP connection (TCP connection) is closed immediately after sending it.
To enable BGP routing, participating routers must have BGP enabled and be assigned to an autonomous system and the neighbor (peer) relationships must be specified. A router typically belongs to only one AS. TCP connections must be established in order for neighbors to exchange routing information and updates. Neighbors exchange BGP open messages that includes information such as AS numbers, BGP versions, router IDs, and hold-time values. Keepalive messages determine if a connection is established and operational. The hold-time value specifies the maximum time BGP will wait between successive messages (either keep alive or update) from its peer, before closing the connection.

In BGP, peers are arranged into groups. A group must contain at least one neighbor. A neighbor must belong to a group. Groups allow multiple peers to share similar configuration attributes.

Although neighbors do not have to belong to the same AS, they must be able to communicate with each other. If TCP connections are not established between two neighbors, the BGP peering will not be established and updates will not be exchanged.

Peer relationships are defined by configuring the IP address of the routers that are peers of the local BGP system. When neighbor and peer relationships are configured, the BGP peers exchange Update messages to advertise network reachability information.
Hierarchical Levels

BGP parameters are initially applied on the global level. These parameters are inherited by the group and neighbor (peer) levels. Parameters can be modified and overridden on a level-specific basis. BGP command hierarchy consists of three levels:

- Global level
- Group level
- Neighbor level

Many of the hierarchical BGP commands can be modified on different levels. The most specific value is used. That is, a BGP group-specific command takes precedence over a global BGP command. A neighbor-specific statement takes precedence over a global BGP and group-specific command; for example, if you modify a BGP neighbor-level command default, the new value takes precedence over group- and global-level settings.

NOTE: Careful planning is essential to implement commands that can affect the behavior of global, group, and neighbor-levels. Because the BGP commands are hierarchical, analyze the values that can disable features on the global or group levels that must be enabled at the neighbor level. For example, if you enable the damping command on the global level but want it disabled only for a specific neighbor (not for all neighbors within the group), you cannot configure a double-no command (no no damping) to enable the feature.

---

Route Reflection

In a standard BGP configuration, all BGP speakers within an AS must have full BGP mesh to ensure that all externally learned routes are redistributed through the entire AS. IBGP speakers do not re-advertise routes learned from one IBGP peer to another IBGP peer. If a network grows, scaling issues could emerge because of the full mesh configuration requirement. Instead of peering with all other IBGP routers in the network, each IBGP router only peers with a router configured as a route reflector.

Route reflection circumvents the full mesh requirement but maintains the full distribution of external routing information within an AS. Route reflection is effective in large networks because it is manageable, scalable, and easy to implement. Route reflection is implemented in autonomous systems with a large internal BGP mesh to reduce the number of IBGP sessions required within an AS.

A large AS can be sub-divided into one or more clusters. Each cluster contains at least one route reflector which is responsible for redistributing route updates to all clients. Route reflector clients do not need to maintain a full peering mesh between each other. They only require a peering to the
route reflector(s) in their cluster. The route reflectors must maintain a full peering mesh between all non-clients within the AS.

Each route reflector must be assigned a cluster ID and specify which neighbors are clients and which are non-clients to determine which neighbors should receive reflected routes and which should be treated as a standard IBGP peer. Additional configuration is not required for the route reflector besides the typical BGP neighbor parameters.

Figure 20 displays a simple full-mesh configuration with several BGP routers. When SR-A receives a route from SR-1 (an external neighbor), it must advertise route information to all of its IBGP peers (SR-B, SR-C, SR-D, etc). To prevent loops, IBGP learned routes are not re-advertised to other IBGP peers.
When route reflectors are configured, the routers within a cluster do not need to be fully meshed. Figure 20 depicts a fully meshed network and Figure 21 depicts the same network but with route reflectors configured to minimize the IBGP mesh between SR-A, SR-B, SR-C, and SR-D. SR-A, configured as the route reflector, is responsible for redistributing route updates to clients SR-B, SR-C, and SR-D. IBGP peering between SR-B, SR-C and SR-D is not necessary because even IBGP learned routes are reflected to the route reflector’s clients.

In Figure 21, SR-E and SR-F are shown as non-clients of the route reflector. As a result, a full mesh of IBGP peerings must be maintained between, SR-A, SR-E and SR-F.

![Figure 21: BGP Configuration with Route Reflectors](image)

When a route reflector receives an advertised route, it selects the best path. If the best path was received from an EBGP peer then it is typically advertised, with next hop unchanged, to all clients and non-client peers of the route reflector. If the best path was received from a non-client peer then it is advertised to all clients of the route reflector. If the best path was received from a client then it is advertised to all clients and non-client peers.
Fast External Failover

Fast external failover on a group and neighbor basis is supported. For eBGP neighbors, this feature controls whether the router should drop an eBGP session immediately upon an interface-down event, or whether the BGP session should be kept up until the hold-time expires.

When fast external failover is disabled, the eBGP session stays up until the hold-time expires or the interface comes back up. If the BGP routes become unreachable as a result of the down IP interface, BGP withdraws the associated routes towards other peers.

Sending of BGP Communities

The capability to explicitly enable or disable the sending of the BGP community attribute to BGP neighbors, other than through the use of policy statements, is supported.

This feature allows an administrator to enable or disable the sending of BGP communities to an associated peer. This feature overrides communities that are already associated with a given route or that may have been added via an export route policy. In other words, even if the export policies leave BGP communities attached to a given route, when the disable-communities feature is enabled, no BGP communities are advertised to the associated BGP peers.
**BGP Route Tunnel**

BGP-tunnel defines a method to distribute MPLS labels associated with a route advertisement. BGP speakers exchanging routes piggyback a label based on Multi-protocol Extensions Attribute. The label is encoded in the NLRI field and SAFI is used to indicate that the NLRI contains a label. Labeled route update is only exchanged between BGP speakers supporting AFI/SAFI for MPLS Label Capability.

BGP speakers not adjacent to each other may choose LDP or RSVP-TE tunnels to reach the next-hop of a BGP labeled route next-hop. Client applications using BGP tunnels must push two labels (BGP label and LDP/RSVP label) on top of the existing label stack (which will typically include one or more service-specific labels) in order to reach the BGP next-hop. The next-hop BGP node can either resolve its own local LDP or RSVP LSPs to reach its next-hop for BGP tunnel, or it may terminate locally.

If BGP speaker nodes are adjacent to each other (for example, ASBRs running EBGP session) and have exchange labeled routes, then only the BGP route label is used to forward traffic towards the next-hop node. If the BGP route tunnel transits through multiple AS, then each AS segment would have two labels. The last BGP segment ASBR may select to have either one (LDP/RSVP) or two (BGP + LDP/RSVP) labels to reach far-end.

**ECMP and BGP Route Tunnels**

ECMP is only available for BGP route tunnels and not the transport LSP that is used to resolve BGP next-hop. If multiple LSP next-hops are available, then only the first next-hop is used and the rest ignored.

**Layer 2 Services and BGP Route Tunnel**

MPLS transport tunnel per VPLS/VLL instance is enabled by an explicit MPLS-SDP configuration for each far-end PE. For BGP-AD based VPLS, SDP must be manually configured to reach the far-end.

**BGP Route Tunnel SDP Binding**

BGP route tunnel based SDP binding is allowed for VPLS and VLL services. Any service using BGP SDP must presume a two label stack to compute SDP MTU.
BGP Overview

BGP Route Tunnel Based BGP-AD Support

LDP is the only supported transport method with pw-template.

BGP Route Tunnel with multi-hop eBGP session

Either RSVP-TE or LDP LSP can be used to resolve the next-hop between two ASBR nodes. The "transport-tunnel" CLI command can be used to select the specific transport LSP method. The "mpls" option under "transport-tunnel" will enable the option to allow either RSVP-TE LSP or LDP LSP. Availability of RSVP-TE LSP is checked at higher priority. If RSVP-TE LSP is not available then LDP LSP is selected.
RSVP-TE LSP Shortcut for BGP Next-Hop Resolution

RSVP-TE shortcut for BGP next-hop resolution is enabled by entering the `config>router>bgp>igp-shortcut rsvp` command at the BGP protocol level.

This command instructs BGP to search for the best metric RSVP LSP to the /32 address of the BGP next-hop. This address can correspond to the system interface or to another loopback used by the BGP instance on the remote node as its router-id. The LSP metric is provided by MPLS in the tunnel table.

In order to provide fallback from RSVP-TE LSP shortcut to an LDP LSP shortcut and then to the IGP next-hop, the above new command is extended to support the following options:

`config>router>bgp>igp-shortcut [ldp | rsvp-te | mpls][disallow-igp]`

The `ldp` option instructs BGP to search for an LDP LSP with a FEC prefix corresponding to the /32 address of the BGP next-hop. This deprecates the existing `ldp-shortcut` command under BGP. Support for the older command will be provided over a number of releases to allow old config files to execute.

The `rsvp-te` option instructs BGP to search for the best metric RSVP LSP to the /32 address of the BGP next-hop. This address can correspond to the system interface or to another loopback used by the BGP instance on the remote node as its router-id. The LSP metric is provided by MPLS in the tunnel table.

The `mpls` option instructs BGP to first attempt to resolve the BGP next-hop to an RSVP LSP. If no RSVP LSP exists or if the existing ones are down, BGP will automatically search for the LDP LSP with a FEC prefix corresponding to the same /32 prefix in the tunnel table and will resolve the BGP next-hop to it.

The `disallow-igp` option also deprecates the existing one under BGP. It continues to work transparently regardless of which type of LSP shortcut, RSVP or LDP, is being used by BGP at any given time. When this option is enabled and if an LSP shortcut of the configured type is not available, the IGP next-hop route will not be used for the BGP next-hop resolution.

---

Core IPv4 Prefix Resolution

The recursive lookup of an IPv4 prefix in RTM will result first in the BGP next-hop determination for the packet’s prefix and then the IGP next-hop resolution for the BGP next-hop prefix. When the `igp-shortcut rsvp-te` option is enabled in BGP, the IGP resolution for the BGP next-hop will provide the best metric RSVP LSP to the BGP next-hop address as the next-hop shortcut. This RSVP shortcut next-hop is installed as a route in the ingress IOM tunnel table.
When an IPv4 packet for this prefix is received on an ingress network interface, a subscriber IES interface, or a regular IES interface, the ingress IOM lookup of the packet will result in sending the packet labeled with the label stack corresponding to the NHLFE of the RSVP LSP.

The failure of a used RSVP LSP shortcut triggers a new resolution which will result in installing a new route in the ingress IOM tunnel table over another RSVP LSP shortcut if available, or an LDP LSP if the `igp-shortcut mpls` option is enabled, or a regular IP next-hop if the `disallow-igp` option is disabled.

---

**Handling of Control Packets**

All control plane packets that require an RTM lookup and whose destination is reachable over a BGP next-hop resolved to an RSVP shortcut will be forwarded over the shortcut. This effectively excludes the vast majority of control packets which have destinations within an autonomous system. The exceptions are for locally generated or in transit ICMP ping and trace route messages for destinations outside of the local autonomous system.
BGP Confederations

In a standard BGP configuration, all BGP speakers, within an autonomous system (AS), have a full mesh of BGP peerings to ensure all externally learned routes are redistributed throughout the entire AS. This is due to the fact that IBGP speakers do not re-advertise routes learned from one IBGP peer to another IBGP peer. However, as a network grows, scaling issues emerge due to the full mesh requirement. The BGP confederation feature is one method to alleviate the full mesh requirement while still maintaining the full distribution of external routing information within an AS; another method that has already been discussed is to use route reflectors.

To form BGP confederations, an AS is logically divided into smaller groupings called sub-confederations. Each sub-confederation must maintain a full mesh of IBGP peerings between all its members (or use route reflection).

The structure of the BGP confederation is not visible to outside autonomous systems. All confederation specific path attributes are stripped from route updates before they are advertised to external BGP peers.

Sub-confederation ASs have EBGP-type peers to other sub-confederation ASs within the confederation. They exchange routing updates as if they were using IBGP. Parameter values such as next hop, metric, and local preference settings are preserved. The confederation appears and behaves like a single AS.

Confederations have the following characteristics:

- A large AS can be sub-divided into smaller ASs (sub-confederations).
- Inside each smaller AS, routing within each sub-confederation is accomplished via IBGP.
- Confed-EBGP is used to communicate between sub-confederations.
- BGP speakers within a sub-confederation must be fully meshed (or use route reflection).
- Each sub-confederation (member) of the confederation has a different AS number. The AS numbers used are typically in the private AS range of 64512 — 65535.

To configure a 7x50 router to belong to a confederation, the confederation number and the sub-AS numbers that are members of the confederation must be configured using the confederation command in the config>router context. The autonomous system of the router, as configured in the config>router context, should be one of the sub-AS members of the confederation.
BGP Decision Process

When a BGP router has multiple routes to a destination in its RIB-IN the BGP decision process is responsible for deciding which one is the best. Whenever a new route is received (for a prefix) the BGP decision process compares this route to the current best path for that prefix by making a series of comparisons. It determines from this process whether the new path should become the new best path or not. This is the sequence of comparisons performed by 7x50:

1. Select the route with the highest route preference.
2. Select the route with the highest Local Preference (LOCAL_PREF).
3. Select the route with the least number of ASNs in its AS Path (unless as-path-ignore is configured). Note that an AS_SET counts as one ASN.
4. Select the route with the lowest Origin.
5. Select the route with the lowest MED if one the following applies:
   → a. Both routes have the MED attribute and were advertised by the same neighbor AS (leftmost [non-confed] AS in AS_PATH).
   → b. Both routes were advertised by different neighbor AS but always-compare-med without the strict-as option is configured.
   → c. One or both routes do not have the MED but always-compare-med is configured and indicates the MED value to assume for routes that do not have the attribute.
6. Select the route learned from an EBGP peer over the route learned from an IBGP peer.
7. Select the route with the lowest distance between the calculating router and the BGP NEXT_HOP of the route (unless ignore-nh-metric is configured). If the BGP NEXT_HOP is resolved by an RSVP-TE tunnel then the configured tunnel metric is used in place of the actual IGP path cost.
8. Select the route with the lowest Originator ID or received from the peer with the lowest BGP Identifier (unless ignore-router-id is configured, and the routes being compared are EBGP routes).
9. Select the route with the shortest Cluster List. An empty cluster list is considered to have a length of 0.
10. Select the route received from the lowest peer IP address.

Option to Ignore Router ID

RFC 5004 describes that in some cases the comparison of router ID in step 8 results in an unnecessary best path transition that achieves nothing except additional churn and instability. To comply with RFC 5004, a configuration option to skip steps 8-10 when comparing two paths learned from different EBGP neighbors is supported.
To support RFC 5004, the `ignore-router-id` command is available in the `config>router>bgp>best-path-selection` and `config>service>vprn>bgp>best-path-selection` configuration contexts. When this command is present and the current best path to a destination was learned from EBGP peer X with BGP identifier x and a new path is received from EBGP peer Y with BGP identifier y the best path remains unchanged if the new path is equivalent to the current best path up to the BGP identifier comparison and y is less than x.

**Note:** If either the current best path or the new path is from a confed-EBGP peer, or the EBGP-learned paths have been received from the same neighbor (same BGP identifier), then steps 8-10 continue to apply.

---

### always-compare-med Command

By default, the Multi-Exit Discriminator (MED) path attribute is used in the decision process only if both routes in the comparison have the attribute and come from the same neighbor AS. However, these rules can be modified using the `always-compare-med` command.

The `always-compare-med` command without the `strict-as` keyword allows BGP paths to be compared even if they have different neighbor autonomous systems (in this case, if neither zero or infinity is part of the command, the comparison requires both paths to have a MED attribute otherwise, zero or infinity specifies the MED value that should be inferred for paths without the attribute). When the `strict-as` keyword is present, MED is only compared between paths from the same neighbor AS and in this case zero or infinity is mandatory and tells BGP how to interpret paths without a MED attribute.

*Table 14* shows how the MED comparison of two paths is influenced by different forms of the `always-compare-med` command.

**Table 14: MED Comparison with always-compare-med**

<table>
<thead>
<tr>
<th>Command</th>
<th>MED comparison step in decision process</th>
</tr>
</thead>
<tbody>
<tr>
<td>no always-compare-med</td>
<td>Only compare the MED of two paths if they come from the same neighbor-AS and both paths have the MED attribute. Otherwise skip the step.</td>
</tr>
<tr>
<td>always-compare-med</td>
<td>Only compare the MED of two paths (whether or not they are from the same neighbor-AS) if they both have the MED attribute. Otherwise skip the step.</td>
</tr>
<tr>
<td>always-compare-med zero</td>
<td>Always compare the MED of two paths, even if they are from different neighbor-AS. If one or both paths do not have a MED attribute, consider the MED to be zero (best possible value).</td>
</tr>
</tbody>
</table>
Table 14: MED Comparison with always-compare-med (Continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>MED comparison step in decision process</th>
</tr>
</thead>
<tbody>
<tr>
<td>always-compare-med infinity</td>
<td>Always compare MED of two paths, even if they are from different neighbor-AS. If one or both paths do not have a MED attribute, consider the MED to be infinite (worse possible value).</td>
</tr>
<tr>
<td>always-compare-med strict-as zero</td>
<td>Only compare the MED of two paths if they come from the same neighbor-AS. If one or both paths do not have a MED attribute, consider the MED to be zero (best possible value).</td>
</tr>
<tr>
<td>always-compare-med strict-as infinity</td>
<td>Only compare the MED of two paths if they come from the same neighbor-AS. If one or both paths do not have a MED attribute, consider the MED to be infinite (worse possible value).</td>
</tr>
</tbody>
</table>

Option to Ignore Next-Hop Metric

The **ignore-nh-metric** command allows the step comparing the distance to the BGP next-hop to be skipped. When this command is present in the **config>service>vprn** context, it applies to the comparison of two imported BGP-VPN routes. When this command is present in the **config>router:bgp** context, it applies to the comparison of any two BGP routes received by that instance. And when this command is present in the **config>service>vprn:bgp** context, it applies to the comparison of two BGP routes learned from VPRN BGP peers (that is, CE peers). In all cases, this option is useful when there are multiple paths for a prefix that are the same in the IGP cost comparison step of the BGP decision process, and the network administrator wants all of them to be used for forwarding (BGP multipath).
Best External

Best-external is a BGP enhancement that allows a BGP speaker to advertise to its IBGP peers its best “external” route for a prefix/NLRI even when its best overall route for the prefix/NLRI is an “internal” route. This is not possible in a “normal” BGP configuration because the base BGP specification prevents a BGP speaker from advertising a non-best route for a destination.

In certain topologies, best-external can improve convergence times, reduce route oscillation, and allow better loadsharing. This is achieved because routers internal to the AS have knowledge of more exit paths from the AS. Enabling Add-paths on border routers of the AS can achieve a similar result, but Add-paths introduces NLRI format changes that must be supported by BGP peers of the border router, and therefore has more interoperability constraints than best-external (which requires no messaging changes).

Enabling the best-external feature is supported only at the config>router>bgp level. This feature can be enabled/disabled on a per address family basis, with IPv4 and IPv6 as the only options supported initially. Enabling best-external for IPv4 causes the new advertisement rules to apply to both regular IPv4 unicast routes as well as labeled-IPv4 (SAFI4) routes. Similarly, enabling best-external for IPv6 causes the new advertisement rules to apply to both regular IPv6 unicast routes as well as labeled-IPv6 (SAFI4) routes.

The advertise-external command cannot be applied to a route reflector unless client-to-client reflection is disabled (disable-client-reflect in the CLI).

Advertisement Rules with Best External

The advertisement rules when advertise-external is enabled can be summarized as follows:

1. If a router has advertise-external enabled and its best overall route is a route from an IBGP peer then this best route should be advertised to EBGP and confed-EBGP peers, AND the “best external” route should be advertised to IBGP peers. The “best external” route is the one found by running the BGP path selection algorithm on all RIB-IN paths except for those learned from the IBGP peers.

2. If a router has advertise-external enabled and its best overall route is a route from an EBGP peer then this best route should be advertised to EBGP, confed-EBGP, and IBGP peers.

3. If a router has advertise-external enabled and its best overall route is a route from a confed-EBGP peer in member AS X then this best route should be advertised to EBGP, IBGP peers and confed-EBGP peers in a member AS ≠ X AND the “best internal” route should be advertised to confed-EBGP peers in member AS X. The “best internal” route is the one found by running the BGP path selection algorithm on all RIB-IN paths except for those learned from member AS X.
Add-paths is a BGP enhancement that allows a BGP router to advertise multiple distinct paths for the same prefix/NLRI. This provides a number of potential benefits, including reduced routing churn, faster convergence, and better loadsharing.

In order for router A to receive multiple paths per NLRI from peer B, for a particular address family, the BGP capabilities advertisement during session setup indicate that peer B wants to send multiple paths for this address family and router A is willing to receive multiple paths for the address family. Refer to draft-ietf-idr-add-paths-04.txt for details of the add-paths capabilities advertisement.

When the add-paths receive capability for an address family that has been negotiated with a peer, all advertisements and withdrawals of NLRI within that address family by that peer includes a path identifier, as described in draft-ietf-idr-add-paths-04.txt.

The path identifiers have no significance to the receiving peer. If the combination of NLRI and path identifier in an advertisement from a peer is unique (does not match an existing route in the RIB-IN from that peer) then the route is added to the RIB-IN. If the combination of NLRI and path identifier in a received advertisement is the same as an existing route in the RIB-IN from the peer then the new route replaces the existing one. If the combination of NLRI and path identifier in a received withdrawal matches an existing route in the RIB-IN from the peer then that route is removed from the RIB-IN. An UPDATE message carrying an IPv4 NLRI with a path identifier is shown in Figure 22.

![Figure 22: BGP Update Message with Path Identifier for IPv4 NLRI](image)

Add-paths are only supported by the base router BGP instance and the EBGP and IBGP sessions it forms with other add-paths capable peers. The ability to send and receive multiple paths per prefix from to and an add-paths peer is configurable per family, with the supported families being:
• IPv4 (including labeled IPv4 routes)
• VPN-IPv4
• IPv6 (including labeled IPv6 routes)
• VPN-IPv6
Sending Multiple Paths per Prefix to Add-Paths Peers

Path Selection Mode and Parameters

The RIB-IN may have multiple paths for a prefix D. The path selection mode refers to the algorithm used to decide which of these paths to advertise to an add-paths peer. In the current implementation, SR supports only one path selection algorithm—essentially the Add-N algorithm described in draft-ietf-idr-add-paths-guidelines-00.txt, Best Practices for Advertisement of Multiple Paths in BGP. The Add-N algorithm implemented in SROS selects, as candidates for advertisement, the N best overall paths for each prefix, regardless of path type (internal vs. external), degree of difference between the paths or use in forwarding. If this set of N best overall paths includes multiple paths with the same BGP NEXT_HOP only the best route with a particular NEXT_HOP is advertised and the others are suppressed.

In the SROS implementation N is configurable, per address-family, at the BGP instance, group and neighbor levels; N has a minimum value of 1 and a maximum value of 16. For peer P belonging to group G the path selection parameters are based on the neighbor configuration for P else the group configuration for G else the BGP instance configuration.

When add-path is enabled for the VPN-IPv4 (or VPN-IPv6) address family in the base router BGP context only VPN-IP routes in the base router BGP RIB-IN are considered for advertisement to Add-Path peers, if a VPRN’s best route to a destination is a bgp-vpn route imported from the base router and it’s next-best route is a CE-learned BGP route that would be accepted by the VPRN’s VRF export policy this next-best route is not advertised, regardless of the base router’s Add-Path configuration.

Routing Policy

BGP and VRF export policies are applied after path selection is performed. If add-paths is configured to send up to N paths to peer P and an export policy prevents X of the N best paths for prefix D from being advertised to P then only the remaining N-X best paths are sent.

BGP Route Advertisement Rules

Add-paths allows non-best paths to be advertised to a peer but it still complies with basic BGP advertisement rules such as the IBGP split horizon rule: a route learned from an IBGP neighbor cannot be re-advertised to another IBGP neighbor unless the router is configured as a route reflector.

If add-paths is configured to send up to N paths to peer P and X of the N best paths for D cannot be advertised to P due to route advertisement rules then only the remaining N-X routes are advertised.
BGP Fast Reroute

BGP fast reroute is a feature that brings together indirection techniques in the forwarding plane and pre-computation of BGP backup paths in the control plane to support fast reroute of BGP traffic around unreachable/failed next-hops. BGP fast reroute is supported for IPv4, IPv6, 6PE, VPN-IPv4 and VPN-IPv6 VPN routes. The supported scenarios are outlined in Table 15.

Note that information for VPNs is described in the BGP Fast Reroute in a VPRN section of the 7x50 SR OS Services Guide.

Table 15: BGP Fast Reroute Scenarios

<table>
<thead>
<tr>
<th>Ingress Packet</th>
<th>Context</th>
<th>Primary Route</th>
<th>Backup Route</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>GRT or VPRN</td>
<td>IPv4 route with IPv4 next-hop A (resolved by IPv4 route1)</td>
<td>IPv4 route with IPv4 next-hop B (resolved by IPv4 route2)</td>
<td>BGP shortcuts</td>
</tr>
<tr>
<td>IPv4</td>
<td>GRT</td>
<td>IPv4 route with IPv4 next-hop A (resolved by tunnel1, which can be any of the following types: ldp, ldp/rsvp, rsvp)</td>
<td>IPv4 route with IPv4 next-hop B (resolved by tunnel2, which can be any of the following types: ldp, ldp/rsvp, rsvp).</td>
<td>BGP shortcuts</td>
</tr>
<tr>
<td>IPv4</td>
<td>GRT</td>
<td>IPv4 route with IPv4 next-hop A (resolved by IPv4 route1)</td>
<td>IPv4 route with IPv4 next-hop B (resolved by tunnel2, which can be any of the following types: ldp, ldp/rsvp, rsvp).</td>
<td>BGP shortcuts</td>
</tr>
<tr>
<td>IPv6</td>
<td>GRT or VPRN</td>
<td>IPv6 route with IPv6 next-hop A (resolved by IPv6 route1)</td>
<td>IPv6 route with IPv6 next-hop B (resolved by IPv6 route2)</td>
<td>BGP shortcuts</td>
</tr>
<tr>
<td>IPv6</td>
<td>GRT</td>
<td>3 IPv6 route with IPv4 next-hop A (resolved by l4route1)</td>
<td>IPv6 route with IPv4 next-hop B (resolved by IPv4 route2)</td>
<td>6over4</td>
</tr>
<tr>
<td>IPv6</td>
<td>GRT</td>
<td>Labeled-IPv6 (6PE) route with IPv4-mapped IPv6 next-hop A (resolved by tunnel1, which can be any of the following types: ldp, ldp/rsvp).</td>
<td>Labeled-IPv6 (6PE) route with IPv4-mapped IPv6 next-hop B (resolved by tunnel2, which can be any of the following types: ldp, ldp/rsvp).</td>
<td>For the best performance the primary and backup next-hops advertise the same label value with all 6PE routes (IPv6 explicit null).</td>
</tr>
<tr>
<td>Ingress Packet</td>
<td>Context</td>
<td>Primary Route</td>
<td>Backup Route</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IPv6</td>
<td>GRT</td>
<td>Labeled-IPv6 (6PE) route with IPv4-mapped IPv6 next-hop A (resolved by tunnel1, which can be any of the following types: ldp, ldp/rsvp).</td>
<td>IPv6 route with IPv6 next-hop B (resolved by IPv6 route2)</td>
<td></td>
</tr>
<tr>
<td>MPLS</td>
<td>Egress</td>
<td>IPv4 route with CE next-hop A (resolved by IPv4 route1)</td>
<td>IPv4 route with CE next-hop B (resolved by IPv4 route2)</td>
<td>VPRN label mode must be VRF.</td>
</tr>
<tr>
<td>MPLS</td>
<td>Egress</td>
<td>IPv6 route with CE next-hop A (resolved by IPv6 route1)</td>
<td>IPv6 route with CE next-hop B (resolved by IPv6 route2)</td>
<td>VPRN label mode must be VRF.</td>
</tr>
<tr>
<td>IPv4</td>
<td>Ingress</td>
<td>VPN-IPv4 route with RD x, PE next-hop A (resolved by tunnel1, which can be any of the following types: gre, ldp, ldp/rsvp, rsvp, bgp/ldp, or bgp/rsvp).</td>
<td>VPN-IPv4 route with RD y, PE next-hop B (resolved by tunnel2, which can be any of the following types: gre, ldp, ldp/rsvp, rsvp, bgp/ldp, or bgp/rsvp).</td>
<td>RD x and RD y can be the same or different. For the best performance the primary and backup next-hops must advertise the same VPRN label value with all routes (e.g. per VRF label).</td>
</tr>
<tr>
<td>IPv6</td>
<td>Ingress</td>
<td>VPN-IPv6 route with RD x, PE next-hop A (resolved by tunnel1, which can be any of the following types: gre, ldp, ldp/rsvp, rsvp, bgp/ldp, or bgp/rsvp).</td>
<td>VPN-IPv6 route with RD y, PE next-hop B (resolved by tunnel2, which can be any of the following types: gre, ldp, ldp/rsvp, rsvp, bgp/ldp, or bgp/rsvp).</td>
<td>RD x and RD y can be the same or different. For the best performance the primary and backup next-hops must advertise the same VPRN label value with all routes (e.g. per VRF label).</td>
</tr>
</tbody>
</table>
Table 15: BGP Fast Reroute Scenarios (Continued)

<table>
<thead>
<tr>
<th>Ingress Packet</th>
<th>Context</th>
<th>Primary Route</th>
<th>Backup Route</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Egress IP VPN PE</td>
<td>IPv4 route with CE next-hop A (resolved by IPv4 route1)</td>
<td>VPN-IPv4 route with RD y, PE next-hop B (resolved by tunnel2, which can be any of the following types: gre, ldp, ldp/rsvp, rsvp, bgp/ldp, or bgp/rsvp).</td>
<td>VPRN label mode must be VRF. VPRN must export its VPN-IP routes with RD ≠ y. For the best performance the backup next-hop must advertise the same VPRN label value with all routes (e.g. per VRF label).</td>
<td></td>
</tr>
<tr>
<td>MPLS Egress IP VPN PE</td>
<td>IPv6 route with CE next-hop A (resolved by IPv6 route1)</td>
<td>VPN-IPv6 route with RD y, PE next-hop B (resolved by tunnel2, which can be any of the following types: gre, ldp, ldp/rsvp, rsvp, bgp/ldp, or bgp/rsvp).</td>
<td>VPRN label mode must be VRF. VPRN must export its VPN-IP routes with RD ≠ y. For the best performance the backup next-hop must advertise the same VPRN label value with all routes (e.g. per VRF label).</td>
<td></td>
</tr>
<tr>
<td>IPv4 Ingress IP VPN PE</td>
<td>VPN-IPv4 route with RD x, PE next-hop A (resolved by tunnel1, which can be any of the following types: gre, ldp, ldp/rsvp, rsvp, bgp/ldp, or bgp/rsvp).</td>
<td>IPv4 route with CE next-hop B (resolved by IPv4 route2)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 23 shows an example of BGP fast reroute in an ingress PE router when a remote PE connected to a multi-homed site is taken out of service.
Calculating Backup Paths

When BGP fast reroute is enabled, the control plane is responsible for selecting one or more primary paths, and if possible, a backup path for each destination IP prefix. The primary paths are the routes tied for best according to the BGP multipath configuration.

The backup path is the single best path remaining after the primary ECMP paths and any paths with the same BGP next-hops as these paths have been removed.

Sending Failure Notifications to the IOM

When BGP fast reroute is enabled, the IOM reroutes traffic onto a backup path based on input from BGP. When BGP decides that a primary path is no longer usable, it sends a message to the IOM indicating that the corresponding BGP next-hop is unreachable/unresolved. If this results in all of the primary paths being unresolved, the IOM switches affected traffic to the backup path.

These are some of the events that can trigger the sending of a next-hop down message to the IOM:

- TCP session closed with the neighbor.
- BGP session terminated with the neighbor.
- Fast-external failover is enabled and the interface with a single-hop EBGP neighbor goes down.
• Peer tracking is enabled and there is no route to the peer address of the neighbor.
• BFD is enabled with a neighbor and the BFD session goes down.
• There is no active IP route that matches the BGP next-hop address.
Command Interactions and Dependencies

This section highlights the BGP command interactions and dependencies which are important for configuration or operational maintenance of the routers. Topics covered in this section are:

- Changing the Autonomous System Number on page 567
- Changing a Confederation Number on page 568
- Changing the Router ID at the Configuration Level on page 568
- Changing the Local AS Number on page 568
- Hold Time and Keep Alive Timer Dependencies on page 569
- Import and Export Route Policies on page 570
- Route Damping and Route Policies on page 570

Note that this information can be found in the BGP Command Reference on page 603 which provides detailed descriptions of the configuration commands.

Changing the Autonomous System Number

If the AS number is changed on a router with an active BGP instance (that is at the config>router>level), the new AS number will not be used until the BGP instance is restarted either by administratively disabling and enabling the BGP instance or by rebooting the system with the new configuration.
Changing the Local AS Number

Changing the local AS of an active BGP instance:

- At the global level causes the BGP instance to restart with the new local AS number.
- At the group level causes BGP to re-establish the peer relationships with all peers in the group with the new local AS number.
- At the neighbor level causes BGP to re-establish the peer relationship with the new local AS number.

Changing a Confederation Number

Changing the a confederation value on an active BGP instance will not restart the protocol. The change will take affect when the BGP protocol is (re) initialized.

Changing the Router ID at the Configuration Level

If you configure a new router ID in the `config>router` context, protocols are not automatically restarted with the new router ID. The next time a protocol is (re) initialized the new router ID is used. An interim period of time can occur when different protocols use different router IDs.
Hold Time and Keep Alive Timer Dependencies

The BGP hold time specifies the maximum time BGP will wait between successive messages (either keep alive or update) from its peer, before closing the connection. This configuration parameter can be set at three levels. The most specific value is used.

- Global level — applies to all peers
- Group level — applies to all peers in group
- Neighbor level — only applies to specified peer

Although the keep alive time can be user specified, the configured keep alive timer is overridden by the value of hold time under the following circumstances:

- If the hold time specified is less than the configured keep alive time, then the operational keep alive time is set to one third of the specified hold time; the configured keep alive time is unchanged.
- If the hold time is set to zero, then the operational value of the keep alive time is set to zero; the configured keep alive time is unchanged. This means that the connection with the peer will be up permanently and no keep alive packets are sent to the peer.

If the hold time or keep alive values are changed, the changed timer values take effect when the new peering relationship is established. Changing the values cause the peerings to restart. The changed timer values are used when re-negotiating the peer relationship.
Import and Export Route Policies

Import and export route policy statements are specified for BGP on the global, group, and neighbor level. Up to five unique policy statement names can be specified in the command line per level. The most specific command is applied to the peer. Defining the policy statement name is not required before being applied. Policy statements are evaluated in the order in which they are specified within the command context.

The import and export policies configured on different levels are not cumulative. The most specific value is used. An import or export policy command specified on the neighbor level takes precedence over the same command specified on the group or global level. An import or export policy command specified on the group level takes precedence over the same command specified on the global level.

Route Damping and Route Policies

To prevent BGP systems from sending excessive route changes to peers, BGP route damping can be implemented. Damping can reduce the number of update messages sent between BGP peers, to reduce the load on peers, without adversely affecting the route convergence time for stable routes.

The damping profile defined in the policy statement is applied to control route damping parameters. Route damping characteristics are specified in a route damping profile and are referenced in the action for the policy statement or in the action for a policy entry. Damping can be specified at the global, group, or neighbor level with the most specific command applied to the peer.

AS Override

AS Override simplifies the use of the same AS number (ASN) across multiple VPRN sites.

The AS Override feature can be used in VPRN scenarios where a customer is running BGP as the PE-CE protocol and some or all of the CE locations are in the same Autonomous System (AS). With normal BGP, two sites in the same AS would not be able to reach each other directly since there is an apparent loop in the ASPATH.

With AS Override enabled on an egress eBGP session, the PE rewrites the customer ASN in the ASPATH with the VPRN AS number as the route is advertised to the CE.
FlowSpec is a standardized method (defined in RFC 5575) for using BGP to distribute traffic flow specifications (flow routes) throughout a network. A flow route carries a description of a flow in terms of packet header fields such as source IP address, destination IP address, or TCP/UDP port number and indicates (through a community attribute) an action to take on packets matching the flow. The primary application for Flowspec is DDoS mitigation.

Flowspec is supported by SROS only by the base router BGP instance and only for IPv4 packets. To exchange IPv4 FlowSpec routes with a BGP peer, the MP-BGP capability for AFI 1 and SAFI 133 must be negotiated when the session is established. The flow-ipv4 keyword must be part of the family command (at the BGP instance, group, or neighbor level) for this capability negotiation to occur.

The NLRI of an IPv4 flow route can contain one or more of the subcomponents shown in Table 16.

<table>
<thead>
<tr>
<th>Subcomponent Name [Type]</th>
<th>Value Encoding</th>
<th>SROS Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IPv4 Prefix [1]</td>
<td>Prefix length, prefix</td>
<td>Yes</td>
</tr>
<tr>
<td>Source IPv4 Prefix [2]</td>
<td>Prefix length, prefix</td>
<td>Yes</td>
</tr>
<tr>
<td>IP Protocol [3]</td>
<td>One or more (operator, value) pairs</td>
<td>Partial. No support for multiple values other than “TCP or UDP”.</td>
</tr>
<tr>
<td>Port [4]</td>
<td>One or more (operator, value) pairs</td>
<td>No</td>
</tr>
<tr>
<td>Destination Port [5]</td>
<td>One or more (operator, value) pairs</td>
<td>Partial. No support for multiple ranges.</td>
</tr>
<tr>
<td>Source Port [6]</td>
<td>One or more (operator, value) pairs</td>
<td>Partial. No support for multiple ranges.</td>
</tr>
<tr>
<td>ICMP Type [7]</td>
<td>One or more (operator, value) pairs</td>
<td>Partial. Only a single value is supported.</td>
</tr>
<tr>
<td>ICMP Code [8]</td>
<td>One or more (operator, value) pairs</td>
<td>Partial. Only a single value is supported.</td>
</tr>
<tr>
<td>TCP Flags [9]</td>
<td>One or more (operator, bitmask) pairs</td>
<td>Partial. Only SYN and ACK flags can be matched.</td>
</tr>
<tr>
<td>Packet Length [10]</td>
<td>One or more (operator, value) pairs</td>
<td>No</td>
</tr>
<tr>
<td>DSCP [11]</td>
<td>One or more (operator, value) pairs</td>
<td>Partial. Only a single value is supported.</td>
</tr>
</tbody>
</table>
Table 16: Subcomponents of IPv4 Flow Route NLRI (Continued)

<table>
<thead>
<tr>
<th>Subcomponent Name [Type]</th>
<th>Value Encoding</th>
<th>SROS Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fragment [12]</td>
<td>One or more (operator, bitmask) pairs</td>
<td>Partial. No support for matching DF bit, first-fragment or last-fragment.</td>
</tr>
</tbody>
</table>

Table 17 summarizes the actions that may be associated with an IPv4 flow route and how each type of action is encoded.

Table 17: IPv4 Flowspec Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Encoding</th>
<th>SROS Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate Limit</td>
<td>Extended community type 0x8006</td>
<td>Partial. Only rate=0 is supported.</td>
</tr>
<tr>
<td>Sample/Log</td>
<td>Extended community type 0x8007. S-bit</td>
<td>Yes</td>
</tr>
<tr>
<td>Next Entry</td>
<td>Extended community type 0x8007. T-bit</td>
<td>No</td>
</tr>
<tr>
<td>Redirect to VRF</td>
<td>Extended community type 0x8008.</td>
<td>Yes</td>
</tr>
<tr>
<td>Mark Traffic Class</td>
<td>Extended community type 0x8009.</td>
<td>No</td>
</tr>
</tbody>
</table>

Note: An IPv4 flow route cannot have more than one instance of a flowspec extended community in the range 0x8006-0x8009. If it has more than one instance, a log/trap is generated and no filter entry is installed for the flow route.

Validating and Importing Received IPv6 Flow Routes into the Routing Table

IPv4 flow routes received from a BGP peer must be validated before being considered for import into the routing table. An IPv4 flow route is considered invalid if:

1. The flow route is received from an EBGP peer and the left most AS number in the AS_PATH attribute does not equal the peer’s AS number (from the group/neighbor configuration).
2. The flowspec-validate command is enabled, the flow route has a destination prefix subcomponent D, and the flow route was received from a peer P that did not advertise the best IP route to D and all more-specific prefixes.

After received flow routes are validated they are processed by the relevant import policies.

Note: An IPv4 flow route never matches a prefix entry in a prefix-list, even if the destination IPv4 prefix subcomponent or the source IPv4 prefix subcomponent of the NLRI is a match.
If the router receives the exact same IPv4 flow route NLRI from multiple peers then the router selects one best path from among all received paths. The best path selection follows the existing implementation (used for all other BGP NLRI). Step 1 of the algorithm eliminates invalid routes and for IPv4 flow routes. This includes routes that were required to meet the validation checks described by the standard but did not. For each NLRI, the route with the best path is:

- Installed in the LOC-RIB.
- Propagated to BGP peers, depending on export policies.
- Used if possible to create an IPv4 filter entry.

---

**Propagating IPv4 Flow Routes to BGP Neighbors**

When the base router BGP instance installs an IPv4 flow route into its LOC-RIB the default export policy causes it to advertise the flow route to all of its AFI=1/SAFI=133 BGP peers.

User-configured export policies can be used to override the default export policy. Export policy actions do not change the contents of the flow route NLRI in any way.

---

**Using IPv4 Flow Routes to Create Dynamic IPv4 Filter Entries**

When the base router BGP instance installs an IPv4 flow route into its LOC-RIB, the system attempts to construct an ipv4-filter entry from the NLRI contents and the action(s) encoded in the UPDATE message. If successful, the filter entry is added to the system-created “fSpec-1” IPv4 filter policy that internally has an identifier of 16777217. This “fSpec-1” filter policy is applied to the following:

- Ingress IPv4 traffic on a network interface, if the `config>router>interface>ingress` configuration includes the keyword flowspec.
- Ingress IPv4 traffic on an IES SAP interface, if the `config>service>ies>interface>sap>ingress` configuration includes the keyword flowspec.
- Ingress IPv4 traffic on an IES spoke SDP interface, if the `config>service>ies>interface>spoke-sdp>ingress` configuration includes the keyword flowspec.
A user-defined IPv4 filter policy can be applied to a base router interface that has IPv4 flow-spec enabled. When an interface has both a user-defined IPv4 filter policy and the system-created ‘fSpec-1’ IPv4 filter policy, the IPv4 filter rules are installed in the following order:

1. User-defined IPv4 filter entries (in ascending order of entry IDs).
2. IPv4 flowspec entries (in order, determined by comparison of the NLRI described in RFC 5575).
TTL Security for LDP

The BGP TTL Security Hack (BTSH) was originally designed to protect the BGP infrastructure from CPU utilization-based attacks. It is derived on the fact that the vast majority of ISP eBGP peerings are established between adjacent routers. Since TTL spoofing is considered nearly impossible, a mechanism based on an expected TTL value can provide a simple and reasonably robust defense from infrastructure attacks based on forged BGP packets.

While TSH is most effective in protecting directly connected peers, it can also provide a lower level of protection to multi-hop sessions. When a multi-hop BGP session is required, the expected TTL value can be set to 255 minus the configured range-of-hops. This approach can provide a qualitatively lower degree of security for BGP (such as a DoS attack could, theoretically, be launched by compromising a box in the path). However, BTSH will catch a vast majority of observed distributed DoS (DDoS) attacks against eBGP. For further information, refer to draft-gill-btsh-xx.txt, The BGP TTL Security Hack (BTSH).

TSH can be used to protect LDP peering sessions as well. For details, see draft-chen-ldp-ttl-xx.txt, TTL-Based Security Option for LDP Hello Message.

The TSH implementation supports the ability to configure TTL security per BGP/LDP peer and evaluate (in hardware) the incoming TTL value against the configured TTL value. If the incoming TTL value is less than the configured TTL value, the packets are discarded and a log is generated.
Figure 24 displays the process to provision basic BGP parameters.

START

CONFIGURE GLOBAL ROUTER PARAMETERS

- CONFIGURE ROUTER ID
- ASSIGN AUTONOMOUS SYSTEM NUMBER
- CONFIGURE CONFEDERATIONS (optional)

CONFIGURE BGP GROUP PARAMETERS

CONFIGURE BGP NEIGHBOR PARAMETERS

TURN UP

Figure 24: BGP Configuration and Implementation Flow
Configuration Notes

This section describes BGP configuration caveats.

General

- Before BGP can be configured, the router ID and autonomous system should be configured.
- BGP must be added to the router configuration. There are no default BGP instances on a router.

BGP Defaults

The following list summarizes the BGP configuration defaults:

- By default, the router is not assigned to an AS.
- A BGP instance is created in the administratively enabled state.
- A BGP group is created in the administratively enabled state.
- A BGP neighbor is created in the administratively enabled state.
- No BGP router ID is specified. If no BGP router ID is specified, BGP uses the router system interface address.
- The router BGP timer defaults are generally the values recommended in IETF drafts and RFCs (see BGP MIB Notes on page 578)
- If no import route policy statements are specified, then all BGP routes are accepted.
- If no export route policy statements specified, then all best and used BGP routes are advertised and non-BGP routes are not advertised.
BGP MIB Notes

The router implementation of the RFC 1657 MIB variables listed in Table 18 differs from the IETF MIB specification.

**Table 18:  and IETF MIB Variations**

<table>
<thead>
<tr>
<th>MIB Variable</th>
<th>Description</th>
<th>RFC 1657 Allowed Values</th>
<th>Allowed Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgpPeerMinASOriginationInterval</td>
<td>Time interval in seconds for the MinASOriginationInterval timer. The suggested value for this timer is 15 seconds.</td>
<td>1 — 65535</td>
<td>2 — 255</td>
</tr>
<tr>
<td>bgpPeerMinRouteAdvertisementInterval</td>
<td>Time interval in seconds for the MinRouteAdvertisementInterval timer. The suggested value for this timer is 30.</td>
<td>1 — 65535</td>
<td>a1 — 255</td>
</tr>
</tbody>
</table>

a. A value of 0 is supported when the rapid-update command is applied to an address family that supports it.

If SNMP is used to set a value of X to the MIB variable in Table 19, there are three possible results:

**Table 19: MIB Variable with SNMP**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>X is within IETF MIB values and X is within SR OS values</td>
<td>SNMP set operation does not return an error MIB variable set to X</td>
</tr>
<tr>
<td>X is within IETF MIB values and X is outside SR OS values</td>
<td>SNMP set operation does not return an error MIB variable set to “nearest” SR OS supported value (e.g., SR OS range is 2 - 255 and X = 65535, MIB variable will be set to 255) Log message generated</td>
</tr>
<tr>
<td>X is outside IETF MIB values and X is outside SR OS values</td>
<td>SNMP set operation returns an error</td>
</tr>
</tbody>
</table>
When the value set using SNMP is within the IETF allowed values and outside the values as specified in Table 18 and Table 19, a log message is generated. The log messages that display are similar to the following log messages:

**Sample Log Message for setting bgpPeerMinASOriginationInterval to 65535**

```
576 2006/11/12 19:45:48 [Snmpd] BGP-4-bgpVariableRangeViolation: Trying to set bgpPeerMinASOrigInt to 65535 - valid range is [2-255] - setting to 255
```

**Sample Log Message for setting bgpPeerMinASOriginationInterval to 1**

```
594 2006/11/12 19:48:05 [Snmpd] BGP-4-bgpVariableRangeViolation: Trying to set bgpPeerMinASOrigInt to 1 - valid range is [2-255] - setting to 2
```

**Sample Log Message for setting bgpPeerMinRouteAdvertisementInterval to 256**

```
535 2006/11/12 19:40:53 [Snmpd] BGP-4-bgpVariableRangeViolation: Trying to set bgpPeerMinRouteAdvInt to 256 - valid range is [2-255] - setting to 255
```

**Sample Log Message for setting bgpPeerMinRouteAdvertisementInterval to 1**

```
566 2006/11/12 19:44:41 [Snmpd] BGP-4-bgpVariableRangeViolation: Trying to set bgpPeerMinRouteAdvInt to 1 - valid range is [2-255] - setting to 2
```
Configuring BGP with CLI

This section provides information to configure BGP using the command line interface.

Topics in this section include:

- BGP Configuration Overview on page 582
  - Preconfiguration Requirements on page 582
  - BGP Hierarchy on page 582
  - Internal and External BGP Configurations on page 582
  - BGP Confederations on page 589
  - BGP Route Reflectors on page 591
- Basic BGP Configuration on page 584
- Common Configuration Tasks on page 586
  - Creating an Autonomous System on page 587
  - Configuring a Router ID on page 588
  - BGP Components on page 593
  - Configuring Group Attributes on page 593
  - Configuring Neighbor Attributes on page 594
  - Configuring Route Reflection on page 595
  - Configuring a Confederation on page 596
- BGP Configuration Management Tasks on page 597
  - Modifying an AS Number on page 597
  - Modifying the BGP Router ID on page 598
  - Deleting a Neighbor on page 600
  - Deleting Groups on page 601
BGP Configuration Overview

Preconfiguration Requirements

Before BGP can be implemented, the following entities must be configured:

- The autonomous system (AS) number for the router.
  
  An AS number is a globally unique value which associates a router to a specific autonomous system. This number is used to exchange exterior routing information with neighboring ASs and as an identifier of the AS itself. Each router participating in BGP must have an AS number specified.
  
  In order to implement BGP, the AS number must be specified in the `config>router` context.

- Router ID — The router ID is the IP address of the local router. The router ID identifies a packet’s origin. The router ID must be a valid host address.

BGP Hierarchy

BGP is configured in the `config>router>bgp` context. Three hierarchical levels are included in BGP configurations:

- Global level
- Group level
- Neighbor level

Commands and parameters configured on the global level are inherited to the group and neighbor levels although parameters configured on the group and neighbor levels take precedence over global configurations.

Internal and External BGP Configurations

A BGP system is comprised of ASs which share network reachability information. Network reachability information is shared with adjacent BGP peers. BGP supports two types of routing information exchanges:

- External BGP (EBGP) is used between ASs.
EBGP speakers peer to different ASs and typically share a subnet. In an external group, the next hop is dependent upon the interface shared between the external peer and the specific neighbor. The `multihop` command must be specified if an EBGP peer is more than one hop away from the local router.

- Internal BGP (IBGP) is used within an AS.

  IBGP peers belong to the same AS and typically does not share a subnet. Neighbors do not have to be directly connected to each other. Since IBGP peers are not required to be directly connected, IBGP uses the IGP path (the IP next-hop learned from the IGP) to reach an IBGP peer for its peering connection.
Basic BGP Configuration

This section provides information to configure BGP and configuration examples of common configuration tasks. The minimal BGP parameters that need to be configured are:

- An autonomous system number for the router.
- A router ID - Note that if a new or different router ID value is entered in the BGP context, then the new value takes precedence and overwrites the router-level router ID.
- A BGP peer group.
- A BGP neighbor with which to peer.
- A BGP peer-AS that is associated with the above peer.

The BGP configuration commands have three primary configuration levels: `bgp` for global configurations, `group name` for BGP group configuration, and `neighbor ip-address` for BGP neighbor configuration. Within the different levels, many of the configuration commands are repeated. For the repeated commands, the command that is most specific to the neighboring router is in effect, that is, neighbor settings have precedence over group settings which have precedence over BGP global settings.

Following is a sample configuration that includes the above parameters. The other parameters shown below are optional:

```plaintext
info
#--------------------------------------------------
echo "IP Configuration"
#--------------------------------------------------
... autonomous-system 200
confederation 300 members 200 400 500 600
router-id 10.10.10.103
#--------------------------------------------------
...#--------------------------------------------------
echo "BGP Configuration"
#--------------------------------------------------
bgp
   graceful-restart
   exit
   cluster 0.0.0.100
   export "direct2bgp"
   router-id 10.0.0.12
   group "To_AS_10000"
   connect-retry 20
   hold-time 90
   keepalive 30
   local-preference 100
   remove-private peer-as 10000
   neighbor 10.0.0.8
description "To_Router B - EBGP Peer"
```
connect-retry 20
hold-time 90
keepalive 30
local-address 10.0.0.12
passive
preference 99
peer-as 10000
exit
exit
group "To_AS_30000"
  connect-retry 20
  hold-time 90
  keepalive 30
  local-address 10.0.0.12
  peer-as 30000
  neighbor 10.0.3.10
    description "To_Router C - EBGP Peer"
    connect-retry 20
    hold-time 90
    keepalive 30
    peer-as 30000
  exit
exit
group "To_AS_40000"
  connect-retry 20
  hold-time 30
  keepalive 30
  local-preference 100
  peer-as 65206
  neighbor 10.0.0.15
    description "To_Router E - Sub Confederation AS 65205"
    connect-retry 20
    hold-time 90
    keepalive 30
    peer-as 65205
  exit
exit
exit
#--------------------------------------------------
....
A:ALA-48>config>router#
This section provides a brief overview of the tasks that must be performed to configure BGP and provides the CLI commands. In order to enable BGP, one AS must be configured and at least one group must be configured which includes neighbor (system or IP address) and peering information (AS number).

All BGP instances must be explicitly created on each router. Once created, BGP is administratively enabled.

Configuration planning is essential to organize ASs and the SRs within the ASs, and determine the internal and external BGP peering.

To configure a basic autonomous system, perform the following tasks:

1. Prepare a plan detailing the autonomous system(s), the router belonging to each group, group names, and peering connections.
2. Associate each router with an autonomous system number.
3. Configure each router with a router ID.
4. Associate each router with a peer group name.
5. Specify the local IP address that will be used by the group or neighbor when communicating with BGP peers.
7. Specify the autonomous system number associated with each neighbor.
Creating an Autonomous System

Before BGP can be configured, the autonomous system must be configured first. In BGP, routing reachability information is exchanged between autonomous systems (ASs). An AS is a group of networks that share routing information. The **autonomous-system** command associates an autonomous system number to the router being configured. The **autonomous-system** command is configured in the `config>router` context.

Use the following CLI syntax to associate a router to an autonomous system:

**CLI Syntax:** `config>router# autonomous-system autonomous-system`

The router series supports 4 bytes AS numbers by default. This means autonomous-system can have any value from 1 to 4294967295. The following example displays autonomous system configuration command usage:

**Example:** `config>router# autonomous-system 100`

The following example displays the autonomous system configuration:

```
ALA-B>config>router# info
#-------------------------------------------------------------
# IP Configuration
#-------------------------------------------------------------
interface "system"
    address 10.10.10.104/32
exit
interface "to-103"
    address 10.0.0.104/24
    port 1/1/1
exit
    autonomous-system 100
#-------------------------------------------------------------
ALA-B>config>router#
```
Configuring a Router ID

In BGP, routing information is exchanged between autonomous systems. The BGP router ID, expressed like an IPv4 address, uniquely identifies the router. It can be set to be the same as the system interface address.

Note that if a new or different router ID value is entered in the BGP context, then the new router ID value is used instead of the router ID configured on the router level, system interface level, or inherited from the MAC address. The router-level router ID value remains intact. The router ID used by BGP is selected in the following order:

- The routed-id configured under `config>router>bgp`
- The router-id configured under `config>router`
- The system interface IPv4 address
- The last 4 bytes of the system MAC address

When configuring a new router ID outside of the `config>router>bgp` context, BGP is not automatically restarted with the new router ID; the next time BGP is (re)initialized the new router ID is used. An interim period of time can occur when different protocols use different router IDs. To force the new router ID, issue the `shutdown` and `no shutdown` commands for BGP or restart the entire router. Use the following CLI syntax to configure the router ID for multiple protocols:

**CLI Syntax:** `config>router# router-id router-id`

The following example displays router ID configuration command usage:

**Example:** `config>router# router-id 10.10.104`

The following example displays the router ID configuration:

```
ALA-B>config>router# info
----------------------------------------------
# IP Configuration
#------------------------------------------
interface "system"
    address 10.10.10.104/32
exit
interface "to-103"
    address 10.0.0.104/24
    port 1/1/1
exit
autonomous-system 100
router-id 10.10.10.104
#------------------------------------------
...
ALA-B>config>router#
```
BGP Confederations

Follow these steps to configure a confederation:

1. Configure the autonomous system number of the confederation using the confederation command in the `config-router` context.
2. Configure the BGP confederation members using the `confederation` command in the `config-router` context.
3. Configure IBGP peering within the (local) sub-confederation.
4. Configure one or more confed-EBGP peerings to peers in other neighboring sub-confederations.

**Figure 25: Confederation Network Diagram Example**

The following configuration displays the minimum BGP configuration for routers in sub-confederation AS 65001 outlined in Figure 26.
ALA-A
config router
  autonomous-system 65001
  confederation 100 members 65001 65002 65003
  bgp
    group confed1
      peer-as 65001
      neighbor 2.2.2.2
      exit
      neighbor 3.3.3.3
      exit
      neighbor 4.4.4.4
      exit
    exit
  group external_confed
    neighbor 5.5.5.5
      peer-as 65002
      exit
    neighbor 9.9.9.9
      peer-as 65003
      exit
    exit
  exit
exit
exit

ALA-D
config router
  autonomous-system 65001
  confederation 100 members 65001 65002 65003
  bgp
    group confed1
      peer-as 65001
      neighbor 1.1.1.1
      exit
      neighbor 2.2.2.2
      exit
      neighbor 3.3.3.3
      exit
    exit
  exit
exit

ROUTER 1
config router
  autonomous-system 65003
  confederation 100 members 65001 65002 65003
  bgp
    group confed1
      peer-as 65001
      neighbor 1.1.1.1
      exit
      neighbor 5.5.5.5
      peer-as 65002
      exit
    exit
  exit
exit
BGP Route Reflectors

In a standard BGP configuration, all BGP speakers within an AS must have a full BGP mesh to ensure that all externally learned routes are redistributed through the entire AS. IBGP speakers do not re-advertise routes learned from one IBGP peer to another IBGP peer. If a network grows, scaling issues could emerge because of the full mesh configuration requirement. Route reflection circumvents the full mesh requirement but still maintains the full distribution of external routing information within an AS.

Autonomous systems using route reflection arrange BGP routers into groups called clusters. Each cluster contains at least one route reflector which is responsible for redistributing route updates to all clients. Route reflector clients do not need to maintain a full peering mesh between each other. They only require a peering to the route reflector(s) in their cluster. The route reflectors must maintain a full peering mesh between all non-clients within the AS.

Each route reflector must be assigned a cluster ID and specify which neighbors are clients and which are non-clients to determine which neighbors should receive reflected routes and which should be treated as a standard IBGP peer. Additional configuration is not required for the route reflector besides the typical BGP neighbor parameters.

Figure 26: Route Reflection Network Diagram Example
The following configuration displays the minimum BGP configuration for routers in Cluster 1.1.1.1 outlined in Figure 26.

ALA-A
  config router bgp
  group cluster1
    peer-as 100
    cluster 1.1.1.1
    neighbor 2.2.2.2
    exit
    neighbor 3.3.3.3
    exit
    neighbor 4.4.4.4
    exit
  exit
  group RRs
    peer-as 100
    neighbor 5.5.5.5
    exit
    neighbor 9.9.9.9
    exit
  exit

ALA-B
  config router bgp
  group cluster1
    peer-as 100
    neighbor 1.1.1.1
  exit
  exit

ALA-C
  config router bgp
  group cluster1
    peer-as 100
    neighbor 1.1.1.1
  exit
  exit

ALA-D
  config router bgp
  group cluster1
    peer-as 100
    neighbor 1.1.1.1
  exit
  exit
BGP Components

Use the CLI syntax displayed below to configure the following BGP attributes:

- BGP Components on page 593
- Configuring Group Attributes on page 593
- Configuring Neighbor Attributes on page 594
- Configuring Route Reflection on page 595
- Configuring a Confederation on page 596

Configuring Group Attributes

A group is a collection of related BGP peers. The group name should be a descriptive name for the group. Follow your group, name, and ID naming conventions for consistency and to help when troubleshooting faults.

All parameters configured for a peer group are applied to the group and are inherited by each peer (neighbor), but a group parameter can be overridden on a specific neighbor-level basis.

The following example displays the BGP group configuration:

```
ALA-B(config-router) bgp# info
----------------------------------------------
...
group "headquarters1"
  description "HQ execs"
  local-address 10.0.0.104
  disable-communities standard extended
  ttl-security 255
  exit
exit

...  
----------------------------------------------
ALA-B(config-router) bgp#
```
Configuring Neighbor Attributes

After you create a group name and assign options, add neighbors within the same autonomous system to create IBGP connections and/or neighbors in different autonomous systems to create EBGP peers. All parameters configured for the peer group level are applied to each neighbor, but a group parameter can be overridden on a specific neighbor basis.

The following example displays neighbors configured in group “headquarters1”.

ALA-B>config>router>bgp# info

```
----------------------------------------------
... 
  group "headquarters1"
    description "HQ execs"
    local-address 10.0.0.104
    disable-communities standard extended
    ttl-security 255
    neighbor 10.0.0.5
      passive
      peer-as 300
    exit
    neighbor 10.0.0.106
      peer-as 100
    exit
    neighbor 17.5.0.2
      hold-time 90
      keepalive 30
      min-as-origination 15
      local-preference 170
      peer-as 10701
    exit
    neighbor 17.5.1.2
      hold-time 90
      keepalive 30
      min-as-origination 15
      local-preference 100
      min-route-advertisement 30
      preference 170
      peer-as 10702
    exit
  exit
...
----------------------------------------------
ALA-B>config>router>bgp#```
Configuring Route Reflection

Route reflection can be implemented in autonomous systems with a large internal BGP mesh to reduce the number of IBGP sessions required. One or more routers can be selected to act as focal points for internal BGP sessions. Several BGP speaking routers can peer with a route reflector. A route reflector forms peer connections to other route reflectors. A router assumes the role as a route reflector by configuring the `cluster cluster-id` command. No other command is required unless you want to disable reflection to specific peers.

If you configure the `cluster` command at the global level, then all subordinate groups and neighbors are members of the cluster. The route reflector cluster ID is expressed in dotted decimal notation. The ID should be a significant topology-specific value. No other command is required unless you want to disable reflection to specific peers.

If a route reflector client is fully meshed, the `disable-client-reflect` command can be enabled to stop the route reflector from reflecting redundant route updates to a client.

The following example displays a route reflection configuration:

```
ALA-B>config>router>bgp# info
---------------------------------------------
cluster 0.0.0.100
  group "Santa Clara"
    local-address 10.0.0.103
    neighbor 10.0.0.91
      peer-as 100
      exit
    neighbor 10.0.0.92
      peer-as 100
      exit
    neighbor 10.0.0.93
      disable-client-reflect
      peer-as 100
      exit
  exit
---------------------------------------------
ALA-B>config>router>bgp#
```
Configuring a Confederation

Reducing a complicated IBGP mesh can be accomplished by dividing a large autonomous system into smaller autonomous systems. The smaller ASs can be grouped into a confederation. A confederation looks like a single AS to routers outside the confederation. Each confederation is identified by its own (confederation) AS number.

To configure a BGP confederation, you must specify a confederation identifier, an AS number expressed as a decimal integer. The collection of autonomous systems appears as a single autonomous system with the confederation number acting as the “all-inclusive” autonomous system number. Up to 15 members (ASs) can be added to a confederation.

NOTE: The confederation command is configured in the config>router context.

Use the following CLI syntax to configure a confederation:

CLI Syntax: config>router# confederation confed-as-num members member-as-num

When 4-byte AS number support is not disabled on router, the confederation and any of its members can be assigned an AS number in the range from 1 to 4294967295. The following example displays a confederation configuration command usage:

Example: config>router># confederation 1000 members 100 200 300

The following example displays the confederation configuration:

ALA-B>config>router# info
#---------------------------------------------------------------
# IP Configuration
#---------------------------------------------------------------
interface "system"
  address 10.10.10.103/32
exit
interface "to-104"
  shutdown
  address 10.0.0.103/24
  port 1/1/1
exit
autonomous-system 100
confederation 1000 members 100 200 300
router-id 10.10.10.103
#---------------------------------------------------------------
ALA-B>config>router#
BGP Configuration Management Tasks

This section discusses the following BGP configuration management tasks:

- Modifying an AS Number on page 597
- Modifying a Confederation Number on page 598
- Modifying the BGP Router ID on page 598
- Modifying the Router-Level Router ID on page 599
- Deleting a Neighbor on page 600
- Deleting Groups on page 601

Modifying an AS Number

You can modify an AS number on a router but the new AS number will not be used until the BGP instance is restarted either by administratively disabling or enabling the BGP instance or by rebooting the system with the new configuration.

Since the AS number is defined in the `config>router` context, not in the BGP configuration context, the BGP instance is not aware of the change. Re-examine the plan detailing the autonomous system(s), the SRs belonging to each group, group names, and peering connections. Changing an AS number on a router could cause configuration inconsistencies if associated `peer-as` values are not also modified as required. At the group and neighbor levels, BGP will re-establish the peer relationships with all peers in the group with the new AS number.

Use the following CLI syntax to change an autonomous system number:

**CLI Syntax:**
```
config>router# autonomous-system autonomous-system
```

**CLI Syntax:**
```
config>router# bgp
   group name
      neighbor ip-addr
      peer-as asn
```

**Example:**
```
config>router# autonomous-system 400
config>router# bgp
config>router>bgp# group headquarters1
config>router>bgp>group# neighbor 10.10.10.103
config>router>bgp>group# peer-as 400
config>router>bgp>group# exit
```
Modifying a Confederation Number

Modifying a confederation number will cause BGP to restart automatically. Changes immediately take effect.

Modifying the BGP Router ID

Changing the router ID number in the BGP context causes the new value to overwrite the router ID configured on the router level, system interface level, or the value inherited from the MAC address. It triggers an immediate reset of all peering sessions.

Example: config>router:bgp# router-id 10.0.0.123

This example displays the BGP configuration with the BGP router ID specified:

ALA-B>config>router:bgp# info detail
----------------------------------------------
no shutdown
no description
no always-compare-med
ibgp-multipath
  ...
router-id 10.0.0.123
----------------------------------------------
ALA-B>config>router:bgp#
Modifying the Router-Level Router ID

Changing the router ID number in the `config>router` context causes the new value to overwrite the router ID derived from the system interface address, or the value inherited from the MAC address.

When configuring a new router ID, protocols are not automatically restarted with the new router ID. The next time a protocol is (re)initialized the new router ID is used. An interim period of time can occur when different protocols use different router IDs. To force the new router ID, issue the `shutdown` and `no shutdown` commands for each protocol that uses the router ID or restart the entire router.

Use the following CLI syntax to change a router ID:

**CLI Syntax:** `config>router# router-id router-id`

**Example:**
```
config>router# router-id 10.10.10.104
config>router# no shutdown
config>router>bgp# shutdown
config>router>bgp# no shutdown
```

The following example displays the router ID configuration:

```
ALA-A>config>router# info
#------------------------------------------
# IP Configuration
#------------------------------------------
interface "system"
   address 10.10.10.104/32
exit
interface "to-103"
   address 10.0.0.104/24
   port 1/1/1
exit
autonomous-system 100
router-id 10.10.10.104
#------------------------------------------
ALA-B>config>router#
```
Deleting a Neighbor

In order to delete a neighbor, you must shut down the neighbor before issuing the `no neighbor ip-addr` command.

Use the following CLI syntax to delete a neighbor:

**CLI Syntax:**
```plaintext
config>router# bgp
    group name
        no neighbor ip-address
        shutdown
        no peer-as asn
        shutdown
```

**Example:**
```plaintext
config>router# bgp
cfg-router>bgp# group headquarters1
config-router>bgp>group# neighbor 10.0.0.103
config-router>bgp>group>neighbor# shutdown
config-router>bgp>group>neighbor# exit
config-router>bgp>group# no neighbor 10.0.0.103
```

The following example displays the “headquarters1” configuration with the neighbor 10.0.0.103 removed.

```plaintext
ALA-B>config>router>bgp# info
-----------------------------------------------
group "headquarters1"
    description "HQ execs"
    local-address 10.0.0.104
    neighbor 10.0.0.5
        passive
        peer-as 300
    exit
exit
-----------------------------------------------
ALA-B>config>router>bgp#
```
Deleting Groups

In order to delete a group, the neighbor configurations must be shut down first. After each neighbor is shut down, you must shut down the group before issuing the `no group name` command.

Use the following CLI syntax to shut down a peer and neighbor and then delete a group:

**CLI Syntax:**
```cli
config>router# bgp
   no group name
   shutdown
   no neighbor ip-address
   shutdown
   shutdown
```

**Example:**
```cli
config>router# bgp
config>router>bgp# group headquarters1
config>router>bgp>group# neighbor 10.0.0.105
config>router>bgp>group>neighbor# shutdown
config>router>bgp>group>neighbor# exit
config>router>bgp>group# neighbor 10.0.0.103
config>router>bgp>group# shutdown
config>router>bgp>group# exit
config>router>bgp# no group headquarters1
```

If you try to delete the group without shutting down the peer-group, the following message appears:

```
ALA-B>config>router>bgp# no group headquarters1
MINOR: CLI BGP Peer Group should be shutdown before deleted. BGP Peer Group not deleted.
```
BGP Command Reference

Command Hierarchies

Configuration Commands

- Global BGP Commands on page 603
- Group BGP Commands on page 606
- Neighbor BGP Commands on page 608
- Show Commands on page 610
- Clear Commands on page 610
- Debug Commands on page 611

```
config
  — router [router-name]
    — confederation [confed-as-num members as-number... (up to 15 max)]
    — no confederation [confed-as-num members as-number... (up to 15 max)]
    — [no] mh-primary-interface [interface-name]
      — [no] address [ip-address/mask | ip-address netmask]
      — [no] description description-string
      — [no] shutdown
    — [no] mh-secondary-interface [interface-name]
      — [no] address [ip-address/mask | ip-address netmask]
      — [no] description description-string
      — [no] shutdown
      — [no] hold-time holdover-time
    — [no] mh-secondary-interface
    — router-id [id-address]
    — no router-id
    — [no] bgp
      — [no] add-paths
        — [no] ipv4 send send-limit receive [none]
        — [no] ipv4 send send-limit
        — [no] ipv4
        — [no] ipv6 send send-limit receive [none]
        — [no] ipv6 send send-limit
        — [no] ipv6
        — [no] vpn-ipv4 [send send-limit receive [none]]
        — [no] vpn-ipv4 end send-limit
        — [no] vpn-ipv4
        — [no] vpn-ipv6 send send-limit receive [none]
        — [no] vpn-ipv6 end send-limit
        — [no] vpn-ipv6
      — [no] advertise-external [ipv4] [ipv6]
      — [no] advertise-inactive
      — [no] aggregator-id-zero
```
— authentication-key [authentication-key | hash-key] [hash | hash2]
— no authentication-key
— auth-keychain name
— backup-path [ipv4] [vpn-ipv4]
— best-path-selection
  — always-compare-med {zero | infinity}
  — always-compare-med strict-as {zero | infinity}
  — no always-compare-med
  — as-path-ignore [ipv4] [vpn-ipv4] [mcast-ipv4] [mvpn-ipv4] [l2-vpn]
  — as-path-ignore
  — ignore-nh-metric
  — ignore-router-id
— [no] bfd-enable
— cluster cluster-id
— no cluster
— connect-retry seconds
— no connect-retry
— [no] damping
— description description-string
— no description
— [no] disable-4byte-asn
— [no] disable-client-reflect
— disable-communities [standard] [extended]
— no disable-communities
— [no] disable-fast-external-failover
— [no] enable-inter-as-vpn
— [no] enable-peer-tracking
— export policy-name [policy-name…](up to 5 max)]
— no export
— family [ipv4] [vpn-ipv4] [mcast-ipv4] [l2-vpn] [mvpn-ipv4] [mdt-safi] [ms-pw] [flow-ipv4] [route-target] [mcast-vpn-ipv4]
— no family
— [no] flowspec-validate
— [no] graceful-restart
— [no] stale-routes-time time
  — no stale-routes-time
— hold-time seconds [min seconds2]
— no hold-time
— [no] ibgp-multipath
— igp-shortcut [ldp | rsvp-te | mpls] [disallow-igp]
— no igp-shortcut
— import policy-name [policy-name ...(up to 5 max)]
— no import
— keepalive seconds
— no keepalive
— local-as as-number [private]
— no local-as
— local-preference local-preference
— no local-preference
— loop-detect {drop-peer | discard-route | ignore-loop | off}
— no loop-detect
— med-out {number | igp-cost}
— no med-out
— min-as-origination seconds
— no min-as-origination
— min-route-advertisement seconds
— no min-route-advertisement
— [no] mp-bgp-keep
— multihop ttl-value
— no multihop
— multipath max-paths
— no multipath
— next-hop-resolution
  — policy policy-name
  — no policy
  — [no] use-bgp-routes
— [no] outbound-route-filtering
  — [no] extended-community
    — [no] accept-orf
    — send-orf [comm-id...(up to 32 max)]
    — no send-orf comm-id
— [no] path-mtu-discovery
— preference preference
— no preference
— purge-timer minutes
— no purge-timer
— [no] rapid-update {[l2-vpn] [mvpn-ipv4] [mde-safi]}
— [no] rapid-withdrawal
— [no] remove-private {limited} {skip-peer-as}
— route-target-list comm-id [comm-id...(up to 15 max)]
— no route-target-list [comm-id]
— router-id ip-address
— no router-id
— [no] shutdown
— transport-tunnel ldp | rsvp-te | mpls
— [no] vpn-apply-export
— [no] vpn-apply-import
config
  — router [router-name]
  — [no] bgp
    — [no] group name
    — [no] add-paths
      — ipv4 send send-limit receive [none]
      — ipv4 send send-limit
      — no ipv4
      — ipv6 send send-limit receive [none]
      — ipv6 end send-limit
      — no ipv6
      — vpn-ipv4 [send send-limit receive [none]
      — vpn-ipv4 end send-limit
      — no vpn-ipv4
      — vpn-ipv6 send send-limit receive [none]
      — vpn-ipv6 end send-limit
      — no vpn-ipv6
    — [no] advertise-inactive
    — [no] aggregator-id-zero
    — authentication-key [authentication-key | hash-key] [hash | hash2]
    — no authentication-key
    — auth-keychain name
    — [no] bfd-enable
    — cluster cluster-id
    — no cluster
    — connect-retry seconds
    — no connect-retry
    — [no] damping
    — description description-string
    — no description
    — [no] disable-4byte-asn
    — [no] disable-client-reflect
    — disable-communities [standard] [extended]
    — no disable-communities
    — [no] disable-fast-external-failover
    — [no] enable-peer-tracking
    — export policy-name [policy-name...(up to 5 max)]
    — no export
    — family [ipv4] [vpn-ipv4] [mcast-ipv4] [l2-vpn] [mvpn-ipv4] [flow-ipv4]
                     [mdt-safi] [mcast-vpn-ipv4]
    — no family
    — [no] flowspec-validate
    — [no] graceful-restart
      — stale-routes-time time
      — no stale-routes-time
    — hold-time seconds [strict]
    — no hold-time
    — import policy-name [policy-name ...(up to 5 max)]
    — no import
    — keepalive seconds
    — no keepalive
    — local-address ip-address
    — no local-address
— local-as as-number [private]
— no local-as
— local-preference local preference
— no local-preference
— loop-detect {drop-peer | discard-route | ignore-loop | off}
— no loop-detect
— med-out {number | igp-cost}
— no med-out
— min-as-origination seconds
— no min-as-origination
— min-route-advertisement seconds
— no min-route-advertisement
— multihop ttl-value
— no multihop
— [no] next-hop-self {ipv4 [vpn-ipv4] [ipv6] [mcast-ipv4] [l2-vpn]} [multihoming primary-anycast secondary-anycast]
— [no] outbound-route-filtering
  — [no] extended-community
  — [no] accept-orf
  — send-orf [comm-id...(up to 32 max)]
  — no send-orf [comm-id]
— [no] passive
— [no] path-mtu-discovery
— peer-as as-number
— no peer-as
— preference preference
— no preference
— prefix-limit limit [log-only] [threshold percent]
— no prefix-limit
— [no] remove-private {limited | skip-peer-as}
— [no] shutdown
— ttl-security min-ttl-value
— no ttl-security
— type {internal | external}
— no type
— [no] updated-error-handling
— [no] vpn-apply-export
— [no] vpn-apply-import
BGP Command Reference

```bash
config
    — router [router-name]
        — [no] bgp
            — [no] group name
            — [no] neighbor ip-address
                — [no] add-paths
                    — ipv4 send send-limit receive [none]
                    — ipv4 send send-limit
                    — no ipv4
                    — ipv6 send send-limit receive [none]
                    — ipv6 end send-limit
                    — no ipv6
                    — vpn-ipv4 [send send-limit receive [none]]
                    — vpn-ipv4 end send-limit
                    — no vpn-ipv4
                    — vpn-ipv6 send send-limit receive [none]
                    — vpn-ipv6 end send-limit
                    — no vpn-ipv6
                — [no] advertise-inactive
                — advertise-label [ipv4]
                — [no] advertise-label
                — [no] aggregator-id-zero
                — auth-keychain name
                — authentication-key [authentication-key | hash-key] [hash | hash2]
                — no authentication-key
                — [no] bfd-enable
                — cluster cluster-id
                — no cluster
                — connect-retry seconds
                — no connect-retry
                — damping
                — description description-string
                — no description
                — [no] disable-4byte-asn
                — [no] disable-client-reflect
                — disable-communities [standard] [extended]
                — no disable-communities
                — [no] disable-fast-external-failover
                — [no] enable-peer-tracking
                — export policy-name [policy-name ...(up to 5 max)]
                — no export
                — family [ipv4] [vpn-ipv4] [mcast-ipv4] [12-vpn] [mvpn-ipv4] [flow-ipv4] [mdt-safi] [route-target] [mcast-vpn-ipv4]
                    — no family
                — [no] flowspec-validate
                — [no] graceful-restart
                    — stale-routes-time time
                    — no stale-routes-time
                — hold-time seconds [strict]
                — no hold-time
                — import policy-name [policy-name ...(up to 5 max)]
                — no import
                — keepalive seconds
```
— no keepalive
— local-address ip-address
— no local-address
— local-as as-number [private]
— no local-as
— local-preference local-preference
— no local-preference
— loop-detect {drop-peer | discard-route | ignore-loop | off}
— no loop-detect
— med-out {number | igp-cost}
— no med-out
— min-as-origination seconds
— no min-as-origination
— min-route-advertisement seconds
— no min-route-advertisement
— multihop ttl-value
— no multihop
— [no] next-hop-self
— [no] outbound-route-filtering
  — [no] extended-community
    — [no] accept-orf
      — send-orf [comm-id...(up to 32 max)]
    — no send-orf [comm-id]
— [no] passive
— [no] path-mtu-discovery
— peer-as as-number
— no peer-as
— preference preference
— no preference
— prefix-limit limit [log-only] [threshold percent]
— no prefix-limit
— [no] remove-private {limited} {skip-peer-as}
— [no] shutdown
— ttl-security min-ttl-value
— no ttl-security
— type {internal | external}
— no type
— [no] updated-error-handling
— [no] vpn-apply-export
— [no] vpn-apply-import

Other BGP-Related Commands

config
  — router [router-name]
    — autonomous-system as-number
    — no autonomous-system
    — router-id ip-address
    — no router-id
Show Commands

```
show
  — router [router-instance]
  — bgp
    — auth-keychain keychain-name
    — damping [damp-type] [detail]
    — damping [ip-prefix] [prefix-length] [detail]
    — group [name] [detail]
    — neighbor [ip-address] [detail]
    — neighbor [as-number] [detail]
    — neighbor ip-address [family type mvpn-type] filter1 [brief]
    — neighbor ip-address [family] filter2
    — neighbor as-number [family] filter2
    — neighbor ip-address orf [filter3]
    — neighbor ip-address graceful-restart
    — next-hop [family] [ip-address] [detail]
    — paths
    — route-target
    — routes [family] [brief]
    — routes [family] prefix [detail | longer | hunt [brief]]
    — routes [family] prefix [detail | longer | hunt [brief]]
    — routes [family type mvpn-type] community comm-id
    — routes [family type mvpn-type] aspath-regex reg-ex
    — routes mvpn-ipv4 type mvpn-type {rd rd | originator-ip ip-address | source-ip ip-address | group-ip ip-address | source-as as-number} [hunt | detail]
    — routes [family type l2vpn-type] [brief]
    — routes [family type l2vpn-type] community comm-id
    — routes [family type l2vpn-type] aspath-regex reg-ex
    — routes l2-vpn l2vpn-type {rd rd | site-id site-id | veid veid | offset vpls-base-offset}
    — routes mdt-safi [rd rd] [grp-address mcast-grp-address] [brief]
    — routes ms-pw [rd rd] [aii-type2 aii-type2] [brief]
    — routes flow-ipv4
    — summary [all]
    — summary [family family] [neighbor ip-address]
```

Clear Commands

```
clear
  — router
  — bgp
    — damping [prefix/ip-prefix-length] [neighbor ip-address] | {group name}
    — flap-statistics [prefix/mask] [neighbor ip-address] | [group group-name] | [regex reg-exp | policy policy-name]
    — neighbor ip-address | as as-number | external | all | soft | soft-inbound
    — neighbor ip-address | as as-number | external | all | statistics
    — neighbor ip-address end-of-rib
    — protocol
```
Debug Commands

```
dbg  —  router
    —  bgp
        —  events [neighbor ip-address | group name]
        —  no events
        —  graceful-restart [neighbor ip-address | group name]
        —  no graceful-restart
        —  keepalive [neighbor ip-address | group name]
        —  no keepalive
        —  notification [neighbor ip-address | group name]
        —  no notification
        —  open [neighbor ip-address | group name]
        —  no open
        —  [no] outbound-route-filtering
        —  packets [neighbor ip-address | group name]
        —  no packets
        —  route-refresh [neighbor ip-address | group name]
        —  no route-refresh
        —  rtm [neighbor ip-address | group name]
        —  no rtm
        —  socket [neighbor ip-address | group name]
        —  no socket
        —  timers [neighbor ip-address | group name]
        —  no timers
        —  update [neighbor ip-address | group name]
        —  no update
```
Configuration Commands

Generic Commands

shutdown

Syntax [no] shutdown

Context config>router>bgp
     config>router>bgp>group
     config>router>bgp>group>neighbor

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

The no form of this command administratively enables an entity.

Unlike other commands and parameters where the default state is not indicated in the configuration file, the shutdown and no shutdown states are always indicated in system generated configuration files.

Default administrative states for services and service entities are described in Special Cases.

The no form of the command places an entity in an administratively enabled state.

Special Cases

BGP Global — The BGP protocol is created in the no shutdown state.

BGP Group — BGP groups are created in the no shutdown state.

BGP Neighbor — BGP neighbors/peers are created in the no shutdown state.
description

Syntax    description description-string
          no description

Context   config>router:bgp
          config>router:bgp>group
          config>router:bgp>group>neighbor

Description This command creates a text description stored in the configuration file for a configuration context.
The no form of the command removes the description string from the context.

Default No description is associated with the configuration context.

Parameters  string — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
BGP Commands

bgp

Syntax  [no] bgp
Context  config>router
Description  This command creates the BGP protocol instance and BGP configuration context. BGP is administratively enabled upon creation.

The no form of the command deletes the BGP protocol instance and removes all configuration parameters for the BGP instance. BGP must be shutdown before deleting the BGP instance. An error occurs if BGP is not shutdown first.

add-paths

Syntax  [no] add-paths
Context  config>router>bgp
         config>router>bgp>group
         config>router>bgp>group>neighbor
Description  This command allows adds the add-paths node to be the configured for one or more families configuration of the BGP instance, a group or a neighbor. The BGP add-paths capability allows the router to send and/or receive multiple paths per prefix to/from a peer. The add-paths command without additional parameters is equivalent to removing Add-Paths support for all address families, which causes sessions that previously negotiated the add-paths capability for one or more address families to go down and come back up without the add-paths capability.

The no form of the command (no add-paths) removes add-paths from the configuration of BGP, the group or the neighbor, causing sessions established using add-paths to go down and come back up without the add-paths capability.

Default  no add-paths
ipv4

Syntax ipv4 send send-limit receive [none]
ipv4 send send-limit
no ipv4

Context config>router:bgp>add-paths
cfg>router:bgp>group>add-paths
cfg>router:bgp>group>neighbor>add-paths

Description This command is used to configure the add-paths capability for IPv4 routes (including labeled IPv4 routes). By default, add-paths is not enabled for IPv4 routes.

The maximum number of paths per IPv4 prefix to send is the configured send limit, which is a mandatory parameter. The capability to receive multiple paths per prefix from a peer is configurable using the receive keyword, which is optional. If the receive keyword is not included in the command the receive capability is enabled by default. Entering the command without optional parameters negotiates the ability to both send and receive multiple paths per IPv4 prefix with each peer and configures the router to send the two best paths per prefix to each peer using the default Add-N, N=2 path selection algorithm.

The no form of the command disables add-paths support for IPv4 routes, causing sessions established using add-paths for IPv4 to go down and come back up without the add-paths capability.

Default no ipv4

Parameters send send-limit — The maximum number of paths per IPv4 prefix that are allowed to be advertised to add-paths peers (the actual number of advertised routes may be less depending on the next-hop diversity requirement, other configuration options, route policies and/or route advertisement rules).

Values 1 — 16, none

receive — The router negotiates the add-paths receive capability for VPN-IPv4 routes with its peers

none — The router does not negotiate the Add-Paths receive capability for VPN-IPv64 routes with its peers.

ipv6

Syntax ipv6 send send-limit receive [none]
ipv6 send send-limit
no ipv6

Context config>router:bgp>add-paths
cfg>router:bgp>group>add-paths
cfg>router:bgp>group>neighbor>add-paths

Description This command is used to configure the add-paths capability for IPv6 routes (including 6PE routes). By default, add-paths is not enabled for IPv6 routes.
The maximum number of paths per IPv6 prefix to send is the configured send-limit, which is a mandatory parameter. The capability to receive multiple paths per prefix from a peer is configurable using the receive keyword, which is optional. If the receive keyword is not included in the command the receive capability is enabled by default.

The no form of the command disables add-paths support for IPv6 routes, causing sessions established using add-paths for IPv6 to go down and come back up without the add-paths capability.

**Default**

```plaintext
no ipv6
```

**Parameters**

```plaintext
send send-limit — The maximum number of paths per IPv6 prefix that are allowed to be advertised to add-paths peers (the actual number of advertised routes may be less depending on the next-hop diversity requirement, other configuration options, route policies and/or route advertisement rules).
```

**Values**

```plaintext
1 — 16, none
```

```plaintext
receive — The router negotiates the add-paths receive capability for VPN-IPv6 routes with its peers
```

```plaintext
none — The router does not negotiate the Add-Paths receive capability for VPN-IPv6 routes with its peers.
```

**vpn-ipv4**

```
Syntax

```plaintext
vpn-ipv4 send send-limit receive [none]
```

```plaintext
vpn-ipv4 send send-limit
```

```plaintext
no vpn-ipv4
```

**Context**

```plaintext
config>router:bgp:add-paths
cfg>router:bgp:group:add-paths
cfg>router:bgp:group:neighbor:add-paths
```

**Description**

This command is used to configure the add-paths capability for VPN-IPv4 routes. By default, add-paths is not enabled for VPN-IPv4 routes.

The maximum number of paths per VPN-IPv4 NLRI to send is the configured send-limit, which is a mandatory parameter. The capability to receive multiple paths per prefix from a peer is configurable using the receive keyword, which is optional. If the receive keyword is not included in the command the receive capability is enabled by default.

The no form of the command disables add-paths support for VPN-IPv4 routes, causing sessions established using add-paths for VPN-IPv4 to go down and come back up without the add-paths capability.

**Default**

```plaintext
no vpn-ipv4
```

**Parameters**

```plaintext
send-limit — The maximum number of paths per VPN-IPv4 NLRI that are allowed to be advertised to add-paths peers (the actual number of advertised routes may be less depending on the next-hop diversity requirement, other configuration options, route policies and/or route advertisement rules).
```

**Values**

```plaintext
1 — 16, none
```

```plaintext
receive — The router negotiates the add-paths receive capability for VPN-IPv4 routes with its peers
```

```plaintext
none — The router does not negotiate the Add-Paths receive capability for VPN-IPv6 routes with its peers.
```
vpn-ipv6

Syntax

```
vpn-ipv6 send send-limit receive [none]
vpn-ipv6 send send-limit
no vpn-ipv6
```

Context

```
config>router:bgp>add-paths
config>router:bgp>group>add-paths
config>router:bgp>group>neighbor>add-paths
```

Description

This command is used to configure the add-paths capability for VPN-IPv6 routes. By default, add-paths is not enabled for VPN-IPv6 routes.

The maximum number of paths per VPN-IPv6 NLRI to send is the configured send-limit, which is a mandatory parameter. The capability to receive multiple paths per prefix from a peer is configurable using the `receive` keyword, which is optional. If the `receive` keyword is not included in the command the receive capability is enabled by default.

The `no` form of the command disables add-paths support for VPN-IPv6 routes, causing sessions established using add-paths for VPN-IPv6 to go down and come back up without the add-paths capability.

Default

```
no vpn-ipv6
```

Parameters

```
send-limit — The maximum number of paths per VPN-IPv6 NLRI that are allowed to be advertised to add-paths peers (the actual number of advertised routes may be less depending on the next-hop diversity requirement, other configuration options, route policies and/or route advertisement rules).
```

```
Values 1 — 16, none
```

```
receive — The router negotiates the add-paths receive capability for VPN-IPv6 routes with its peers
```

```
none — The router does not negotiate the add-paths receive capability for VPN-IPv6 routes with its peers.
```

advertise-external

Syntax

```
[no] advertise-external [ipv4] [ipv6]
```

Context

```
config>router:bgp
```

Description

This command allows BGP to advertise its best external route to a destination even when its best overall route is an internal route. Entering the command (or its no form) with no address family parameters is equivalent to specifying all supported address families.

The no form of the command disables Advertise Best External for the BGP family.

Default

```
no advertise-external
```

Parameters

```
ipv4 — Enable/disable best-external advertisement for all IPv4 (unicast and labeled-unicast) routes.
```

```
ipv6 — Enable/disable best-external advertisement for all IPv6 (unicast and labeled-unicast) routes.
```
advertise-inactive

Syntax  
[no] advertise-inactive

Context  
config>router:bgp  
config>router:bgp>group  
config>router:bgp>group>neighbor

Description  
This command enables the advertising of inactive BGP routes to other BGP peers. By default, BGP only advertises BGP routes to other BGP peers if a given BGP route is chosen by the route table manager as the most preferred route within the system and is active in the forwarding plane. This command allows system administrators to advertise a BGP route even though it is not the most preferred route within the system for a given destination.

The no form of the command disables the advertising of inactive BGP routers to other BGP peers.

Default  
no advertise-inactive

advertise-label

Syntax  
advertise-label [ipv4]  
no advertise-label

Context  
config>router:bgp>group>neighbor

Description  
This command configures the IPv4 transport peers to exchange prefixes using 6PE, as well as RFC 3107-labeled IPv4 routes.

If ipv4 is enabled all IPv4 routes advertised to the remote BGP peer will be sent with an RFC 3107-formatted label for the destination route.

The no form of the command disables any or all configured options.

The command must include one or more of the options above.

Default  
no advertise-label

Parameters  
ipv4 — Specifies the advertisement label address family for core IPv4 routes. This keyword can be specified only for an IPv4 peer.

aggregator-id-zero

Syntax  
[no] aggregator-id-zero

Context  
config>router:bgp  
config>router:bgp>group  
config>router:bgp>group>neighbor

Description  
This command is used to set the router ID in the BGP aggregator path attribute to zero when BGP aggregates routes. This prevents different routers within an AS from creating aggregate routes that contain different AS paths.
When BGP is aggregating routes, it adds the aggregator path attribute to the BGP update messages. By default, BGP adds the AS number and router ID to the aggregator path attribute.

When this command is enabled, BGP adds the router ID to the aggregator path attribute. This command is used at the group level to revert to the value defined under the global level, while this command is used at the neighbor level to revert to the value defined under the group level.

The `no` form of the command used at the global level reverts to default where BGP adds the AS number and router ID to the aggregator path attribute.

The `no` form of the command used at the group level reverts to the value defined at the global level.

The `no` form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

*no aggregator-id-zero* — BGP adds the AS number and router ID to the aggregator path attribute.

### always-compare-med

**Syntax**

- `always-compare-med {zero | infinity}`
- `no always-compare-med strict-as {zero | infinity}`
- `no always-compare-med`

**Context**

- `config>router>bgp>best-path-selection`
- `config>service>vprn>bgp>best-path-selection`

**Description**

This command configures the comparison of BGP routes based on the MED attribute. The default behavior of SR-OS (equivalent to the `no` form of the command) is to only compare two routes on the basis of MED if they have the same neighbor AS (the first non-confed AS in the received AS_PATH attribute), and they both have a MED attribute. The `always-compare-med` command without the `strict-as` keyword allows BGP paths to be compared even if they have different neighbor AS (in this case, if neither `zero` or `infinity` is part of the command, the comparison requires both paths to have a MED attribute, otherwise, `zero` or `infinity` specifies the MED value that should be inferred for paths without the attribute. When the `strict-as` keyword is present, MED is only compared between paths from the same neighbor AS, and in this case, `zero` or `infinity` is mandatory and tells BGP how to interpret paths without a MED attribute.

The `no` form of the command removes the parameter from the configuration.

**Default**

*no always-compare-med* — Only compare MEDs of routes that have the same peer AS.

**Parameters**

- `zero` — Specifies that for routes learned without a MED attribute that a zero (0) value is used in the MED comparison. The routes with the lowest metric are the most preferred.
- `infinity` — Specifies for routes learned without a MED attribute that a value of infinity (2^32-1) is used in the MED comparison. This in effect makes these routes the least desirable.
- `strict-as` — Specifies BGP paths to be compared even with different neighbor AS.
as-path-ignore

Syntax

```
as-path-ignore [ipv4] [vpn-ipv4] [mcast-ipv4] [mvpn-ipv4] [l2-vpn]
no as-path-ignore
```

Context

```
config>router:bgp>best-path-selection
config>service>vprn:bgp>best-path-selection
```

Description

This command determines whether the AS path is used to determine the best BGP route. If this option is present, the AS paths of incoming routes are not used in the route selection process. The no form of the command removes the parameter from the configuration.

Default

```
no as-path-ignore
```

Parameters

- **ipv4** — Specifies that the AS-path length will be ignored for all IPv4 routes.
- **vpn-ipv4** — Specifies that the lengthAS-path will be ignored for all IPv4 VPRN routes.
- **mcast-ipv4** — Specifies that the AS-path length will be ignored for all IPv4 multicast routes.
- **mvpn-ipv4** — Specifies that the AS-path length will be ignored for all mVPN IPv4 multicast routes.
- **l2-vpn** — The AS-path length will be ignored for all L2-VPN NLRIs.

auth-keychain

Syntax

```
auth-keychain name
```

Context

```
config>router:bgp
config>router:bgp>group
config>router:bgp>group>neighbor
```

Description

This command configures a TCP authentication keychain to use for the session. The keychain allows the rollover of authentication keys during the lifetime of a session.

Default

```
no auth-keychain
```

Parameters

- **name** — Specifies the name of the keychain, up to 32 characters, to use for the specified TCP session or sessions.

authentication-key

Syntax

```
authentication-key [authentication-key | hash-key] [hash | hash2]
no authentication-key
```

Context

```
config>router:bgp
config>router:bgp>group
config>router:bgp>group>neighbor
```

Description

This command configures the BGP authentication key.
Authentication is performed between neighboring routers before setting up the BGP session by verifying the password. Authentication is performed using the MD-5 message-based digest.

The authentication key can be any combination of ASCII characters up to 255 characters long.

The no form of the command reverts to the default value.

**Default**

MD5 Authentication is disabled by default.

**Parameters**

- **authentication-key** — The authentication key. The key can be any combination of ASCII characters up to 255 characters in length (unencrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

- **hash-key** — The hash key. The key can be any combination of ASCII characters up to 342 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

- **hash** — Specifies the key is entered in an encrypted form. If the hash parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the hash parameter specified.

- **hash2** — Specifies the key is entered in a more complex encrypted form. If the hash2 parameter is not used, the less encrypted hash form is assumed.

**backup-path**

**Syntax**

```
backup-path [ipv4]
no backup-path [ipv4] [ipv6]
```

**Context**

```
config>router:bgp
config>service>vprn:bgp
```

**Description**

This command enables the computation and use of a backup path for IPv4 and/or IPv6 BGP routes belonging to the base router or a particular VPRN. Multiple paths must be received for a route in order to take advantage of this feature. When a route has a backup path and the last of its primary paths (the equal-cost best paths selected by the multipath algorithm) becomes unreachable, traffic matching the route is quickly diverted to the backup path. When many routes share the same set of primary paths and the same backup path, the time to failover traffic to the backup path is independent of the number of routes.

This feature must be enabled in the VRF for BGP FRR (Edge PIC) for VPN-IPV4/V6.

By default, IPv4 and IPv6 routes do not have a backup path installed in the FIB.

**Default**

no backup-path

**Parameters**

- **ipv4** — Enables the use of a backup path for IPv4 BGP routes (excluding labeled IPv4 routes and VPN-IPv4 routes); disable the use of a backup path for IPv4 BGP routes when present in the no form of the command (as in no backup-path ipv4)

- **vpn-ipv4** — Enables the use of a backup path for vpn-ipv4 BGP routes; disables the use of a backup path for vpn-ipv4 BGP routes when present in the no form of the command (as in no backup-path vpn-ipv4)
best-path-selection

**Syntax**

best-path-selection

**Context**

config>router:bgp

**Description**

This command enables path selection configuration.

bfd-enable

**Syntax**

[no] bfd-enable

**Context**

config>router:bgp
config>router:bgp>group
config>router:bgp>group>neighbor

**Description**

This command enables the use of bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated IGP/BGP protocol adjacency.

**Default**

no bfd-enable

cluster

**Syntax**

cluster cluster-id
no cluster

**Context**

config>router:bgp
config>router:bgp>group
config>router:bgp>group>neighbor

**Description**

This command configures the cluster ID for a route reflector server.

Route reflectors are used to reduce the number of IBGP sessions required within an AS. Normally, all BGP speakers within an AS must have a BGP peering with every other BGP speaker in an AS. A route reflector and its clients form a cluster. Peers that are not part of the cluster are considered to be non-clients.

When a route reflector receives a route, first it must select the best path from all the paths received. If the route was received from a non-client peer, then the route reflector sends the route to all clients in the cluster. If the route came from a client peer, the route reflector sends the route to all non-client peers and to all client peers except the originator.

For redundancy, a cluster can have multiple route reflectors.

Confederations can also be used to remove the full IBGP mesh requirement within an AS.

The **no** form of the command deletes the cluster ID and effectively disables the Route Reflection for the given group.
Configuration Commands

Default  
no cluster — No cluster ID is defined.

Parameters  
cluster-id — The route reflector cluster ID is expressed in dot decimal notation.

Values  
Any 32 bit number in dot decimal notation.  (0.0.0.1 — 255.255.255.255)

confederation

Syntax  
confederation confed-as-num members member-as-num

no confederation confed-as-num [members member-as-num]

Context  
config>router

Description  
This command creates confederation autonomous systems within an AS.

This technique is used to reduce the number of IBGP sessions required within an AS. Route reflection is the other technique that is commonly deployed to reduce the number of IBGP sessions.

The no form of the command deletes the specified member AS from the confederation.

When members are not specified in the no statement, the entire list is removed and confederations is disabled.

When the last member of the list is removed, confederations is disabled.

Default  
no confederation — No confederations are defined.

Parameters  
confed-as-num — The confederation AS number expressed as a decimal integer.

Values  
1 — 65535

members member-as-num — The AS number(s) of members that are part of the confederation expressed as a decimal integer. Configure up to 15 members per confed-as-num.

connect-retry

Syntax  
connect-retry seconds

no connect-retry

Context  
config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor

Description  
This command configures the BGP connect retry timer value in seconds.

When this timer expires, BGP tries to reconnect to the configured peer. This configuration parameter can be set at three levels: global level (applies to all peers), peer-group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

The no form of the command used at the global level reverts to the default value.

The no form of the command used at the group level reverts to the value defined at the global level.

The no form of the command used at the neighbor level reverts to the value defined at the group level.

Default  
120 seconds
Parameters

seconds — The BGP Connect Retry timer value in seconds expressed as a decimal integer.

Values 1 — 65535

damping

Syntax [no] damping

Context config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor

Description This command enables BGP route damping for learned routes which are defined within the route policy. Use damping to reduce the number of update messages sent between BGP peers and reduce the load on peers without affecting the route convergence time for stable routes. Damping parameters are set via route policy definition.

The no form of the command used at the global level reverts route damping.
The no form of the command used at the group level reverts to the value defined at the global level.
The no form of the command used at the neighbor level reverts to the value defined at the group level.

When damping is enabled and the route policy does not specify a damping profile, the default damping profile is used. This profile is always present and consists of the following parameters:

- Half-life: 15 minutes
- Max-suppress: 60 minutes
- Suppress-threshold: 3000
- Reuse-threshold: 750

Default no damping — Learned route damping is disabled.

disable-4byte-asn

Syntax [no] disable-4byte-asn

Context config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor

Description This command disables the use of 4-byte ASNs. It can be configured at all 3 level of the hierarchy so it can be specified down to the per peer basis.

If this command is enabled 4-byte ASN support should not be negotiated with the associated remote peer(s).
The no form of the command resets the behavior to the default which is to enable the use of 4-byte ASN.
disable-client-reflect

**Syntax**

```bash
[no] disable-client-reflect
```

**Context**

```bash
config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor
```

**Description**

This command disables the reflection of routes by the route reflector to the clients in a specific group or neighbor.

This only disables the reflection of routes from other client peers. Routes learned from non-client peers are still reflected to all clients.

The **no** form re-enables client reflection of routes.

**Default**

`no disable-client-reflect` — Client routes are reflected to all client peers.

disable-communities

**Syntax**

```bash
disable-communities [standard] [extended]
no disable-communities
```

**Context**

```bash
config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor
```

**Description**

This command configures BGP to disable sending communities.

**Parameters**

- **standard** — Specifies standard communities that existed before VPRNs or 2547.
- **extended** — Specifies BGP communities used were expanded after the concept of 2547 was introduced, to include handling the VRF target.

disable-fast-external-failover

**Syntax**

```bash
[no] disable-fast-external-failover
```

**Context**

```bash
config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor
```

**Description**

This command configures BGP fast external failover.
enable-inter-as-vpn

Syntax  [no] enable-inter-as-vpn

Context  config>router:bgp

Description  This command specifies whether VPNs can exchange routes across autonomous system boundaries, providing model B connectivity.

The no form of the command disallows ASBRs to advertise VPRN routes to their peers in other autonomous systems.

Default  no enable-inter-as-vpn

enable-peer-tracking

Syntax  [no] enable-peer-tracking

Context  config>router:bgp
          config>router:bgp>group
          config>router:bgp>group>neighbor

Description  This command enables BGP peer tracking. BGP peer tracking allows a BGP peer to be dropped immediately if the route used to resolve the BGP peer address is removed from the IP routing table and there is no alternative available. The BGP peer will not wait for the holdtimer to expire; therefore, the BGP reconvergence process is accelerated.

The no form of the command disables peer tracking.

Default  no enable-peer-tracking

export

Syntax  export policy-name [policy-name…]
        no export [policy-name]

Context  config>router:bgp
          config>router:bgp>group
          config>router:bgp>group>neighbor

Description  This command specifies the export route policy used to determine which routes are advertised to peers.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific level is used.

When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of fifteen (15) policy names can be configured. The first policy that matches is applied.

When multiple export commands are issued, the last command entered overrides the previous command.
When no export policies are specified, BGP routes are advertised and non-BGP routes are not advertised by default.

The `no` form of the command removes the policy association with the BGP instance. To remove association of all policies, use the `no export` command without arguments.

**Default**  
`no export` — No export policy is specified. BGP routes are advertised and non-BGP routes are not advertised.

**Parameters**  
`policy-name` — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the `config>router>policy-options` context.

### family

**Syntax**  
`family [ipv4] [vpn-ipv4][mcast-ipv4] [l2-vpn] [mvpn-ipv4] [flow-ipv4] [ms-pw] [route-target] [mcast-vpn-ipv4]`  
`no family`

**Context**  
`config>router:bgp`  
`config>router:bgp>group`  
`config>router:bgp>group>neighbor`

**Description**  
This command specifies the address family or families to be supported over BGP peerings in the base router. This command is additive so issuing the `family` command adds the specified address family to the list.

The `no` form of the command removes the specified address family from the associated BGP peerings. If an address family is not specified, then reset the supported address family back to the default.

**Default**  
`ipv4`

**Parameters**  

`vpn-ipv4` — Exchanges IPv4 VPN routing information.

`mcast-ipv4` — Exchanges multicast IPv4 routing information.

`l2-vpn` — Exchanges Layer 2 VPN information.

`mvpn-ipv4` — Exchanges Multicast VPN related information.

`flow-ipv4` — Exchanges IPv4 flowspec routes belonging to AFI 1 and SAFI 133.

`ms-pw` — Exchanges dynamic MS-PW related information.

`route-target` — Exchanges RT constraint routes for VPN route filtering.

`mcast-vpn-ipv4` — Exchanges Multicast Routes in VPN using SAFI 129.
flowspec-validate

Syntax  
flowspec-validate  
no flowspec-validate

Context  
config>router:bgp  
config>router:bgp>group  
config>router:bgp>group>neighbor

Description  
This command enables/disables validation of received flowspec routes. A flow route with a destination prefix subcomponent received from a particular peer is considered valid if and only if that peer also advertised the best unicast route to the destination prefix and any of its more-specific components. Also, when a flow route is received from an EBGP peer the leftmost AS number in the AS_PATH attribute must equal the peer's AS number. If validation is enabled and a flowspec route is not valid it is not eligible for import into the RIB, it is not used for filtering, a log/trap is generated and it is not propagated to other flowspec peers.

The no form of the command disables the validation procedure.

Default  
no flowspec-validate

route-target-list

Syntax  
route-target-list  
no route-target-list  
comm-id 
comm-id ..[up to 15 max]]

Context  
config>router:bgp

Description  
This command specifies the route target(s) to be accepted and advertised from/to route reflector clients. If the route-target-list is a non-null list, only routes with one or more of the given route targets are accepted or advertised to route reflector clients.

This command is only applicable if the router is a route-reflector server. This parameter has no affect on non-route-reflector clients.

If the route-target-list is assigned at the global level, then the list applies to all route-reflector clients connected to the system.

The no form of the command with a specified route target community, removes the specified community from the route-target-list. The no form of the command entered without a route target community removes all communities from the list.

Default  
no route-target-list

Parameters  
comm-id — Specifies the route target community in the form <0..65535>:<0..65535>
updated-error-handling

Syntax  [no] updated-error-handling

Context  config>router:bgp>group
         config>router:bgp>group>neighbor

Description  This command controls whether SROS utilizes the new neighbor-complete bit when processing optional transitive path attributes and advertising them to the associated BGP neighbor.
This command also control if SROS utilizes the error handling mechanism for optional-transitive path attributes.

Default  no updated-error-handling

vpn-apply-export

Syntax  [no] vpn-apply-export

Context  config>router:bgp
         config>router:bgp>group
         config>router:bgp>group>neighbor

Description  This command causes the base instance BGP export route policies to be applied to VPN-IPv4 routes.
The no form of the command disables the application of the base instance BGP route policies to VPN-IPv4 routes.

Default  no vpn-apply-export

vpn-apply-import

Syntax  [no] vpn-apply-import

Context  config>router:bgp
         config>router:bgp>group
         config>router:bgp>group>neighbor

Description  This command causes the base instance BGP import route policies to be applied to VPN-IPv4 routes.
The no form of the command disables the application of the base instance BGP import route policies to VPN-IPv4 routes.

Default  no vpn-apply-import
graceful-restart

Syntax  
[no] graceful-restart

Context  
config>router:bgp  
config>router:bgp>group  
config>router:bgp>group>neighbor

Description  
This command enables graceful-restart for BGP. When the control plane of a GR-capable router fails, the neighboring routers (GR helpers) temporarily preserve neighbor information, so packets continue to be forwarded through the failed GR router using the last known routes. The helper state remains until the peer completes its restart or exits if the GR timer value is exceeded.

The no form of the command disables graceful restart and removes all graceful restart configurations in the BGP instance.

Default  
o graceful-restart

stale-routes-time

Syntax  
stale-routes-time time  
no stale-routes-time

Context  
config>router:bgp>graceful-restart  
config>router:bgp>group>graceful-restart  
config>router:bgp>group>neighbor>graceful-restart

Description  
This command configures the maximum amount of time in seconds that stale routes should be maintained after a graceful restart is initiated.

The no form of the command resets the stale routes time back to the default of 360 seconds.

Default  
no restart time

Parameters  
time — Specify the amount of time that stale routes should be maintained after a graceful restart is initiated.

Values  
1 — 3600 seconds

Default  
No peer groups are defined.
Configuration Commands

Parameters  

name — The peer group name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

hold-time

Syntax  

hold-time seconds [min seconds2]
no hold-time

Context  

config>router:bgp
config>router:bgp>group
config>router:bgp>group>neighbor

Description  

This command configures the BGP hold time, expressed in seconds.

The BGP hold time specifies the maximum time BGP waits between successive messages (either keepalive or update) from its peer, before closing the connection. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in group) or neighbor level (only applies to specified peer). The most specific value is used.

Even though the implementation allows setting the keepalive time separately, the configured keepalive timer is overridden by the hold-time value under the following circumstances:

1. If the specified hold-time is less than the configured keepalive time, then the operational keepalive time is set to a third of the hold-time; the configured keepalive time is not changed.
2. If the hold-time is set to zero, then the operational value of the keepalive time is set to zero; the configured keepalive time is not changed. This means that the connection with the peer is up permanently and no keepalive packets are sent to the peer.

The no form of the command used at the global level reverts to the default value.
The no form of the command used at the group level reverts to the value defined at the global level.
The no form of the command used at the neighbor level reverts to the value defined at the group level.

Default  

90 seconds

Parameters  

seconds — The hold-time, in seconds, expressed as a decimal integer. A value of 0 indicates the connection to the peer is up permanently.

Values  

0, 3 — 65535

seconds2 — The minimum hold-time that will be accepted for the session. If the peer proposes a hold-time lower than this value, the session attempt will be rejected.

ibgp-multipath

Syntax  

[no] ibgp-multipath

Context  

config>router:bgp

Description  

This command enables IBGP multipath load balancing when adding BGP routes to the route table if the route resolving the BGP nexthop offers multiple nexthops.
The **no** form of the command disables the IBGP multipath load balancing feature.

**Default**  
no ibgp-multipath

### ignore-nh-metric

**Syntax**  
ignore-nh-metric  
no ignore-nh-metric

**Context**  
config>router>bgp>best-path-selection  
config>service>vprn  
config>service>vprn>bgp>best-path-selection

**Description**  
This command instructs BGP to disregard the resolved distance to the BGP next-hop in its decision process for selecting the best route to a destination. When configured in the config>router>bgp>best-path-selection context, this command applies to the comparison of two BGP routes with the same NLRI learned from base router BGP peers. When configured in the config>service>vprn context, this command applies to the comparison of two BGP-VPN routes for the same IP prefix imported into the VPRN from the base router BGP instance. When configured in the config>service>vprn>bgp>best-path-selection context, this command applies to the comparison of two BGP routes for the same IP prefix learned from VPRN BGP peers.

The **no** form of the command (no ignore-nh-metric) restores the default behavior whereby BGP factors distance to the next-hop into its decision process.

**Default**  
no ignore-nh-metric

### ignore-router-id

**Syntax**  
ignore-router-id  
no ignore-router-id

**Context**  
config>router>bgp>best-path-selection  
config>service>vprn>bgp>best-path-selection

**Description**  
When the ignore-router-id command is present and the current best path to a destination was learned from EBGP peer X with BGP identifier x and a new path is received from EBGP peer Y with BGP identifier y the best path remains unchanged if the new path is equivalent to the current best path up to the BGP identifier comparison – even if y is less than x. The **no** form of the command restores the default behavior of selecting the route with the lowest BGP identifier (y) as best.

**Default**  
no ignore-router-id
igp-shortcut

**Syntax**

```plaintext
igp-shortcut [ldp | rsvp-te | mpls] [disallow-igp]
no igp-shortcut
```

**Context**

`config>router>bgp`

**Description**

This command enables the use of LDP tunnels, RSVP tunnels, or both, to resolve paths to BGP next-hops. The `ldp` option instructs BGP to search for an LDP LSP with a FEC prefix corresponding to the /32 address of the BGP next-hop. This deprecates the existing ldp-shortcut command under BGP. Support for the older command will be provided over a number of releases to allow old config files to execute.

The `rsvp-te` option instructs BGP to search for the best metric RSVP LSP to the /32 address of the BGP next-hop. This address can correspond to the system interface or to another loopback used by the BGP instance on the remote node as its router-id. The LSP metric is provided by MPLS in the tunnel table.

The `mpls` option instructs BGP to first attempt to resolve the BGP next-hop to an RSVP LSP. If no RSVP LSP exists or if the existing ones are down, BGP will automatically search for the LDP LSP with a FEC prefix corresponding to the same /32 prefix in the tunnel table and will resolve the BGP next-hop to it.

The `disallow-igp` option also deprecates the existing one under BGP. It continues to work transparently regardless of which type of LSP shortcut, RSVP or LDP, is being used by BGP at any given time. When this option is enabled and if an LSP shortcut of the configured type is not available, the IGP next-hop route will not be used for the BGP next-hop resolution.

**Default**

`no igp-shortcut`

**Parameters**

- `ldp` — Enables the use of LDP LSPs for BGP next-hop resolution by BGP.
- `rsvp-te` — Enables the use of RSVP LSPs for BGP next-hop resolution by BGP.
- `mpls` — Enables the use of both RSVP and LDP LSPs for BGP next-hop resolution by BGP. RSVP LSPs are preferred.
- `disallow-igp` — Prevents BGP next-hop resolution to a regular IGP next-hop if no LSP shortcut was found.

import

**Syntax**

```plaintext
import policy-name [policy-name…]
no import [policy-name]
```

**Context**

`config>router>bgp`

- `config>router>bgp>group`
- `config>router>bgp>group>neighbor`

**Description**

This command specifies the import route policy to be used to determine which routes are accepted from peers. Route policies are configured in the `config>router>policy-options` context.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific level is used.

When multiple policy names are specified, the policies are evaluated in the order they are specified. A maximum of fifteen (15) policy names can be specified. The first policy that matches is applied.
When multiple `import` commands are issued, the last command entered will override the previous command.

When an import policy is not specified, BGP routes are accepted by default.

The `no` form of the command removes the policy association with the BGP instance. To remove association of all policies, use `no import` without arguments.

**Default**

no import — No import policy specified (BGP routes are accepted).

**Parameters**

policy-name — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the `config>router>policy-options` context.

---

**keepalive**

**Syntax**

keepalive seconds  
no keepalive

**Context**

config>router:bgp  
config>router:bgp>group  
config>router:bgp>group>neighbor

**Description**

This command configures the BGP keepalive timer. A keepalive message is sent every time this timer expires.

The `keepalive` parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The `keepalive` value is generally one-third of the `hold-time` interval. Even though the implementation allows the `keepalive` value and the `hold-time` interval to be independently set, under the following circumstances, the configured `keepalive` value is overridden by the `hold-time` value:

1. If the specified `keepalive` value is greater than the configured `hold-time`, then the specified value is ignored, and the `keepalive` is set to one third of the current `hold-time` value.

2. If the specified `hold-time` interval is less than the configured `keepalive` value, then the `keepalive` value is reset to one third of the specified `hold-time` interval.

3. If the `hold-time` interval is set to zero, then the configured value of the `keepalive` value is ignored. This means that the connection with the peer is up permanently and no `keepalive` packets are sent to the peer.

The `no` form of the command used at the global level reverts to the default value
The `no` form of the command used at the group level reverts to the value defined at the global level.

The `no` form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

30 seconds

**Parameters**

seconds — The keepalive timer in seconds expressed as a decimal integer.

**Values**

0 — 21845
Configuration Commands

local-address

Syntax

- **local-address ip-address**
- **no local-address**

Context

- config>router>bgp>group
- config>router>bgp>group>neighbor

Description

This command configures the local IP address used by the group or neighbor when communicating with BGP peers. Outgoing connections use the local-address as the source of the TCP connection when initiating connections with a peer.

When a local address is not specified, the router uses the system IP address when communicating with IBGP peers and uses the interface address for directly connected EBGP peers. This command is used at the neighbor level to revert to the value defined under the group level.

The no form of the command removes the configured local-address for BGP. The no form of the command used at the group level reverts to the value defined at the global level. The no form of the command used at the neighbor level reverts to the value defined at the group level.

Default

- **no local-address** - The router ID is used when communicating with IBGP peers and the interface address is used for directly connected EBGP peers.

Values

- **ipv4-address** — The local address expressed in dotted decimal notation. Allowed value is a valid routable IP address on the router, either an interface or system IP address.

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address: a.b.c.d (host bits must be 0)</td>
</tr>
</tbody>
</table>

local-as

Syntax

- **local-as as-number [private]**
- **no local-as**

Context

- config>router>bgp
- config>router>bgp>group
- config>router>bgp>group>neighbor

Description

This command configures a BGP virtual autonomous system (AS) number.

In addition to the global AS number configured for BGP in the config>router>autonomous-system context, a virtual (local) AS number can be configured to support various AS number migration scenarios. The local AS number is added to the to the beginning the as-path attribute ahead of the router’s AS number.

This configuration parameter can be set at three levels: global level (applies to all EBGP peers), group level (applies to all EBGP peers in peer-group) or neighbor level (only applies to EBGP specified peer). Thus, by specifying this at each neighbor level, it is possible to have a separate local-as per EBGP session. The local-as command is not supported for IBGP sessions. When the optional **private** keyword is specified in the command the local-as number is not added to inbound routes from the EBGP peer that has local-as in effect.

When a command is entered multiple times for the same AS, the last command entered is used in the configuration. The **private** attribute can be added or removed dynamically by reissuing the command.
Changing the local AS at the global level in an active BGP instance causes the BGP instance to restart with the new local AS number. Changing the local AS at the global level in an active BGP instance causes BGP to re-establish the peer relationships with all peers in the group with the new local AS number. Changing the local AS at the neighbor level in an active BGP instance causes BGP to re-establish the peer relationship with the new local AS number.

This is an optional command and can be used in the following circumstance:

Provider router P is moved from AS1 to AS2. The customer router that is connected to P, however, is configured to belong to AS1. To avoid reconfiguring the customer router, the local-as value on router P can be set to AS1. Thus, router P adds AS1 to the as-path message for routes it advertises to the customer router.

The no form of the command used at the global level will remove any virtual AS number configured. The no form of the command used at the group level reverts to the value defined at the global level. The no form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

no local-as

**Parameters**

as-number — The virtual autonomous system number expressed as a decimal integer.

Values

1 — 65535

private — Specifies the local-as is hidden in paths learned from the peering.

---

**local-preference**

**Syntax**

local-preference local-preference

no local-preference

**Context**

config>router:bgp
cfg>router:bgp>group
cfg>router:bgp>group>neighbor

**Description**

This command enables setting the BGP local-preference attribute in incoming routes if not specified and configures the default value for the attribute.

This value is used if the BGP route arrives from a BGP peer without the local-preference integer set.

The specified value can be overridden by any value set via a route policy. This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The no form of the command at the global level specifies that incoming routes with local-preference set are not overridden and routes arriving without local-preference set are interpreted as if the route had local-preference value of 100.

The no form of the command used at the group level reverts to the value defined at the global level.

The no form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

no local-preference — Does not override the local-preference value set in arriving routes and analyze routes without local preference with value of 100.
Parameters

*local-preference* — The local preference value to be used as the override value expressed as a decimal integer.

Values

0 — 4294967295

**loop-detect**

**Syntax**

```plaintext
loop-detect {drop-peer | discard-route | ignore-loop | off}
no loop-detect
```

**Context**

```plaintext
config>router:bgp
cfg-router:bgp>group
config-router:bgp>group>neighbor
```

**Description**

This command configures how the BGP peer session handles loop detection in the AS path.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

Note that dynamic configuration changes of `loop-detect` are not recognized.

The *no* form of the command used at the global level reverts to default, which is `loop-detect ignore-loop`.

The *no* form of the command used at the group level reverts to the value defined at the global level.

The *no* form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

`loop-detect ignore-loop`

**Parameters**

- **drop-peer** — Sends a notification to the remote peer and drops the session.
- **discard-route** — Discards routes received from a peer with the same AS number as the router itself. This option prevents routes looped back to the router from being added to the routing information base and consuming memory. When this option is changed, the change will not be active for an established peer until the connection is re-established for the peer.
- **ignore-loop** — Ignores routes with loops in the AS path but maintains peering.
- **off** — Disables loop detection.

**mdt-safi**

**Syntax**

```plaintext
[no] mdt-safi
```

**Context**

```plaintext
config>router:bgp
cfg-router:bgp>group
config-router:bgp>group>neighbor
```

**Description**

This command enables peer capability to exchange MDT-SAFI address family advertisements.
med-out

**Syntax**
```
med-out {number | igp-cost}
```

**no med-out**

**Context**
```
config>router:bgp
config>router:bgp>group
config>router:bgp>group>neighbor
```

**Description**
This command enables advertising the Multi-Exit Discriminator (MED) and assigns the value used for the path attribute for the MED advertised to BGP peers if the MED is not already set.

The specified value can be overridden by any value set via a route policy.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The `no` form of the command used at the global level reverts to default where the MED is not advertised.

The `no` form of the command used at the group level reverts to the value defined at the global level.

The `no` form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**
```
no med-out
```

**Parameters**
- `number` — The MED path attribute value expressed as a decimal integer.
  - **Values**
    - 0 — 4294967295
- `igp-cost` — The MED is set to the IGP cost of the given IP prefix.

min-as-origination

**Syntax**
```
min-as-origination seconds
```

**no min-as-origination**

**Context**
```
config>router:bgp
config>router:bgp>group
config>router:bgp>group>neighbor
```

**Description**
This command configures the minimum interval, in seconds, at which a path attribute, originated by the local router, can be advertised to a peer.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The `no` form of the command used at the global level reverts to default.

The `no` form of the command used at the group level reverts to the value defined at the global level.

The `no` form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**
```
15 seconds
```
Configuration Commands

**Parameters**

*seconds* — The minimum path attribute advertising interval in seconds expressed as a decimal integer.

**Values**  

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>255</td>
<td></td>
</tr>
</tbody>
</table>

### min-route-advertisement

**Syntax**

`min-route-advertisement seconds`

**no min-route-advertisement**

**Context**

```
config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor
```

**Description**

This command configures the minimum interval, in seconds, at which a prefix can be advertised to a peer.

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The `no` form of the command used at the global level reverts to default.

The `no` form of the command used at the group level reverts to the value defined at the global level.

The `no` form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

30 seconds

**Parameters**

*seconds* — The minimum route advertising interval, in seconds, expressed as a decimal integer.

**Values**  

<table>
<thead>
<tr>
<th>Value</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>255</td>
<td></td>
</tr>
</tbody>
</table>

### multihop

**Syntax**

`multihop ttl-value`

**no multihop**

**Context**

```
config>router>bgp
config>router>bgp>group
config>router>bgp>group>neighbor
```

**Description**

This command configures the time to live (TTL) value entered in the IP header of packets sent to an EBGP peer multiple hops away.

The `no` form of the command is used to convey to the BGP instance that the EBGP peers are directly connected.

The `no` form of the command used at the global level reverts to default.

The `no` form of the command used at the group level reverts to the value defined at the global level.

The `no` form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

1 — EBGP peers are directly connected.

64 — IBGP
Parameters  

*ttl-value* — The TTL value expressed as a decimal integer.

**Values**  
1 — 255

**multipath**

**Syntax**  
multipath integer  
no multipath

**Context**  
config>router:bgp

**Description**  
This command enables BGP multipath.

When multipath is enabled, BGP load shares traffic across multiple links. Multipath can be configured to load share traffic across a maximum of 32 routes. If the equal cost routes available are more than the configured value, then routes with the lowest next-hop IP address value are chosen.

This configuration parameter is set at the global level (applies to all peers).

Multipath is effectively disabled if the value is set to one. When multipath is disabled, and multiple equal cost routes are available, the route with the lowest next-hop IP address will be used.

The no form of the command used at the global level reverts to default where multipath is disabled.

**Default**  
no multipath

**Parameters**  
integer — The number of equal cost routes to use for multipath routing. If more equal cost routes exist than the configured value, routes with the lowest next-hop value are chosen. Setting this value to 1 disables multipath.

**Values**  
1 — 32

**next-hop-resolution**

**Syntax**  
next-hop-resolution

**Context**  
config:bgp

**Description**  
This command enables the context to configure next-hop resolution parameters.

**policy**

**Syntax**  
policy policy-name  
no policy

**Context**  
config>router:bgp>next-hop-res

**Description**  
This command specifies the policy to be applied for filtering the routes to be considered for next-hop resolution process.

The no form of the command removes the policy.
Configuration Commands

**Default**  
no policy

### use-bgp-routes

**Syntax**  
[no] use-bgp-routes

**Context**  
config>router>bgp>next-hop-res

**Description**  
This command specifies whether to use BGP routes to resolve BGP nexthop for IPv4 and IPv6 families on this router instance.

**Default**  
no use-bgp-routes

### outbound-route-filtering

**Syntax**  
[no] outbound-route-filtering

**Context**  
config>router>bgp  
config>router>bgp>group  
config>router>bgp>group>neighbor

**Description**  
This command opens the configuration tree for sending or accepting BGP filter lists from peers (outbound route filtering).

**Default**  
no outbound-route-filtering

### extended-community

**Syntax**  
[no] extended-community

**Context**  
config>router>bgp  
config>router>bgp>group  
config>router>bgp>group>neighbor

**Description**  
The extended-community command opens the configuration tree for sending or accepting extended-community based BGP filters.

In order for the no version of the command to work, all sub-commands (send-orf, accept-orf) must be removed first.

**Default**  
Community filtering is not enabled by default.
**accept-orf**

**Syntax**

```markdown
[no] accept-orf
```

**Context**

```
config>router>bgp
cfg-router>bgp>group
cfg-router>bgp>group>neighbor
```

**Description**

This command instructs the router to negotiate the receive capability in the BGP ORF negotiation with a peer, and to accept filters that the peer wishes to send.

The **no** form of the command causes the router to remove the accept capability in the BGP ORF negotiation with a peer, and to clear any existing ORF filters that are currently in place.

**Default**

Accepting ORFs is not enabled by default.

**send-orf**

**Syntax**

```markdown
send-orf [comm-id...(up to 32 max)]
no send-orf [comm-id]
```

**Context**

```
config>router>bgp
cfg-router>bgp>group
cfg-router>bgp>group>neighbor
```

**Description**

This command instructs the router to negotiate the send capability in the BGP outbound route filtering (ORF) negotiation with a peer.

This command also causes the router to send a community filter, prefix filter, or AS path filter configured as an inbound filter on the BGP session to its peer as an ORF Action ADD.

The **no** form of this command causes the router to remove the send capability in the BGP ORF negotiation with a peer.

The **no** form also causes the router to send an ORF remove action for a community filter, prefix filter, or AS path filter configured as an inbound filter on the BGP session to its peer.

If the **comm-id** parameter(s) are not exclusively route target communities then the router will extract appropriate route targets and use those. If, for some reason, the **comm-id** parameter(s) specified contain no route targets, then the router will not send an ORF.

**Default**

```markdown
no send-orf — Sending ORF is not enabled by default.
```

**Parameters**

- **comm-id** — Any community policy which consists exclusively of route target extended communities. If it is not specified, then the ORF policy is automatically generated from configured route target lists, accepted client route target ORFs and locally configured route targets.
neighbor

Syntax    [no] neighbor ip-address

Context config>router>bgp>group

Description This command creates a BGP peer/neighbor instance within the context of the BGP group.
This command can be issued repeatedly to create multiple peers and their associated configuration.
The no form of the command is used to remove the specified neighbor and the entire configuration associated with the neighbor. The neighbor must be administratively shutdown before attempting to delete it. If the neighbor is not shutdown, the command will not result in any action except a warning message on the console indicating that neighbor is still administratively up.

Default No neighbors are defined.

Parameters  
ip-address — The IP address of the BGP peer router in dotted decimal notation.

Values  ipv4-address: a.b.c.d (host bits must be 0)

next-hop-self

Syntax    [no] next-hop-self { [ipv4] [vpn-ipv4] [ipv6] [mcast-ipv4] [l2-vpn] } [multihoming primary-anycast secondary-anycast] 

Context config>router>bgp>group
config>router>bgp>group>neighbor

Description This command configures the group or neighbor to always set the NEXTHOP path attribute to its own physical interface when advertising to a peer.
This is primarily used to avoid third-party route advertisements when connected to a multi-access network.
In addition, this command can be used to enable and configure the multi-homing resiliency mechanism replacing the usual BGP nexthop with a configured anycast address.
The no form of the command used at the group level allows third-party route advertisements in a multi-access network.
The no form of the command used at the neighbor level reverts to the value defined at the group level.

Default no next-hop-self — Third-party route advertisements are allowed.

Parameters  

vpn-ipv4 — Exchanges IPv4 VPN routing information.

ipv6 — Exchanges IPv6 routing information.

mcast-ipv4 — Exchanges multicast IPv4 routing information.

l2-vpn — Exchanges Layer 2 VPN information.

primary-anycast — Specifies the anycast address that the local node will use to replace the BGP nexthop address in route updates associated peers.
secondary-address — Specifies the anycast address that the local node is to track.

passive

Syntax [no] passive

Context config>router:bgp>group
       config>router:bgp>group>neighbor

Description Enables/disables passive mode for the BGP group or neighbor.

When in passive mode, BGP will not attempt to actively connect to the configured BGP peers but responds only when it receives a connect open request from the peer.

The no form of the command used at the group level disables passive mode where BGP actively attempts to connect to its peers.

The no form of the command used at the neighbor level reverts to the value defined at the group level.

Default no passive — BGP will actively try to connect to all the configured peers.

peer-as

Syntax peer-as as-number

Context config>router:bgp>group
       config>router:bgp>group>neighbor

Description This command configures the autonomous system number for the remote peer. The peer AS number must be configured for each configured peer.

For EBGP peers, the peer AS number configured must be different from the autonomous system number configured for this router under the global level since the peer will be in a different autonomous system than this router.

For IBGP peers, the peer AS number must be the same as the autonomous system number of this router configured under the global level.

This is required command for each configured peer. This may be configured under the group level for all neighbors in a particular group.

Default No AS numbers are defined.

Parameters as-number — The autonomous system number expressed as a decimal integer.

Values 1 — 4294967295
path-mtu-discovery

Syntax  [no] path-mtu-discovery

Context  config>router:bgp
         config>router:bgp>group
         config>router:bgp>group>neighbor

Description  This command enables path MTU discovery for the associated TCP connections. In doing so, the MTU for the associated TCP session will be initially set to the egress interface MTU. The DF bit will also be set so that if a router along the path of the TCP connection cannot handle a packet of a particular size without fragmenting, it will send back an ICMP message to set the path MTU for the given session to a lower value that can be forwarded without fragmenting.

The no form of the command disables path MTU discovery.

Default  no path-mtu-discovery

preference

Syntax  [no] preference preference

Context  config>router:bgp
         config>router:bgp>group
         config>router:bgp>group>neighbor

Description  This command configures the route preference for routes learned from the configured peer(s).

This configuration parameter can be set at three levels: global level (applies to all peers), group level (applies to all peers in peer-group) or neighbor level (only applies to specified peer). The most specific value is used.

The lower the preference the higher the chance of the route being the active route. The router assigns BGP routes highest default preference compared to routes that are direct, static or learned via MPLS or OSPF.

The no form of the command used at the global level reverts to default value.

The no form of the command used at the group level reverts to the value defined at the global level.

The no form of the command used at the neighbor level reverts to the value defined at the group level.

Default  170

Parameters  preference — The route preference expressed as a decimal integer.

Values  1 — 255

purge-timer

Syntax  purge-timer minutes
         no purge-timer

Context  config>router:bgp
Description
When the system sends a VPN-IP Route-Refresh to a peer it sets all the VPN-IP routes received from that peer (in the RIB-IN) to stale and starts the purge-timer. If the routes are not updated (refreshed) before the purge-timer has expired then the routes are removed.

The BGP purge timer configures the time before stale routes are purged.

The no form of the command reverts to the default.

Default 10

Parameters
minutes — Specifies the maximum time before stale routes are purged.

Values 1 — 60

rapid-update

Syntax rapid-update { [l2-vpn] [mvpn-ipv4] [mdt-safi] } 
no rapid-update { [l2-vpn] [mvpn-ipv4] [mdt-safi] }

Context config>router>bgp

Description This command enables and disables BGP rapid update for specified address-families. When no parameter is given for the no rapid-update statement, rapid update is disabled for all address-families.

Default no rapid-update

rapid-withdrawal

Syntax [no] rapid-withdrawal

Context config>router>bgp

Description This command disables the delay (Minimum Route Advertisement) on sending BGP withdrawals. Normal route withdrawals may be delayed up to the minimum route advertisement to allow for efficient packing of BGP updates.

The no form of the command removes this command from the configuration and returns withdrawal processing to the normal behavior.

Default no rapid-withdrawal

prefix-limit

Syntax prefix-limit limit [log-only] [threshold percent] 
no prefix-limit

Context config>router>bgp>group
config>router>bgp>group>neighbor

Description This command configures the maximum number of routes BGP can learn from a peer.
When the number of routes reaches 90% of this limit, an SNMP trap is sent. When the limit is exceeded, the BGP peering is dropped and disabled.

The **no** form of the command removes the **prefix-limit**.

**Parameters**

- **log-only** — Enables the warning message to be sent at the specified threshold percentage, and also when the limit is exceeded. However, the BGP peering is not dropped.
- **percent** — The threshold value (as a percentage) that triggers a warning message to be sent.

**Default**

- **no prefix-limit**

**Parameters**

- **limit** — The number of routes that can be learned from a peer expressed as a decimal integer.

**Values**

- **1** — 4294967295

---

**remove-private**

**Syntax**

```plaintext
[no] remove-private {limited} {skip-peer-as}
```

**Context**

- `config>router:bgp`
- `config>router:bgp>group`
- `config>router:bgp>group>neighbor`

**Description**

This command allows private AS numbers to be removed from the AS path before advertising them to BGP peers.

When the **remove-private** parameter is set at the global level, it applies to all peers regardless of group or neighbor configuration. When the parameter is set at the group level, it applies to all peers in the group regardless of the neighbor configuration.

The router software recognizes the set of AS numbers that are defined by IANA as private. These are AS numbers in the range 64512 through 65535, inclusive.

The **no** form of the command used at the global level reverts to default value. The **no** form of the command used at the group level reverts to the value defined at the global level. The **no** form of the command used at the neighbor level reverts to the value defined at the group level.

**Default**

- **no remove-private** — Private AS numbers will be included in the AS path attribute.

- **limited** — This optional keyword removes private ASNs up to the first public ASN encountered. It then stops removing private ASNs.

- **skip-peer-as** — This optional keyword causes this command to not remove a private ASN from the AS-Path if that ASN is the same as the BGP peer AS number.
router-id

**Syntax**  
router-id *ip-address*  
no router-id

**Context**  
config>router>bgp

**Description**  
This command specifies the router ID to be used with this BGP instance. Changing the BGP router ID on an active BGP instance causes the BGP instance to restart with the new router ID. The router ID must be set to a valid host address.

**Default**  
No router-id is configured for BGP by default. The system interface IP address is used.

**Parameters**  
*ip-address* — The router ID expressed in dotted decimal notation. Allowed value is a valid routable IP address on the router, either an interface or system IP address. It is highly recommended that this address be the system IP address.

split-horizon

**Syntax**  
[no] split-horizon

**Context**  
config>router>bgp>group *group-name*>neighbor *ip-int-name*

**Description**  
This command enables the use of split-horizon. Split-horizon prevents routes from being reflected back to a peer that sends the best route. It applies to routes of all address families and to any type of sending peer; confed-EBGP, EBGP and IBGP. The configuration default is no split-horizon, meaning that no effort is taken to prevent a best route from being reflected back to the sending peer.

**NOTE:** Use of the split-horizon command may have a detrimental impact on peer and route scaling and therefore operators are encouraged to use it only when absolutely needed.

**Default**  
no split-horizon

transport-tunnel

**Syntax**  
transport-tunnel *ldp* | *rsvp-te* | *mpls*

**Context**  
config>router>bgp

**Description**  
This command selects the transport LSP option to provide model B or C connectivity. The no form of the command defaults to LDP as transport LSP method for model B or C connectivity.
Default transport-tunnel ldp

Parameters

- ldp — Allows LDP-based LSPs to be used as transport from the ASBR to local PE routers.
- rsvp-te — Allows RSVP-TE based LSPs to be used as transport from the ASBR to local PE routers.
- mpls — Specifies that both LDP and RSVP-TE can be used to resolve the BGP next-hop for VPRN routes in an associated VPRN instance.

**ttl-security**

Syntax

```
ttl-security min-ttl-value
no ttl-security
```

Context

```
config>router:bgp>group
config>router:bgp>group>neighbor
```

Description

This command configures TTL security parameters for incoming packets. When the feature is enabled, BGP/LDP will accept incoming IP packets from a peer only if the TTL value in the packet is greater than or equal to the minimum TTL value configured for that peer.

The `no` form of the command disables TTL security.

Parameters

- `min-ttl-value` — Specify the minimum TTL value for an incoming packet.

Values

- 1 — 255

Default

- 1

**type**

Syntax

```
[no] type {internal | external}
```

Context

```
config>router:bgp>group
config>router:bgp>group>neighbor
```

Description

This command designates the BGP peer as type internal or external.

The type of `internal` indicates the peer is an IBGP peer while the type of external indicates that the peer is an EBGP peer.

By default, the router derives the type of neighbor based on the local AS specified. If the local AS specified is the same as the AS of the router, the peer is considered `internal`. If the local AS is different, then the peer is considered `external`.

The `no` form of the command used at the group level reverts to the default value.

The `no` form of the command used at the neighbor level reverts to the value defined at the group level.

Default

- `no type` — Type of neighbor is derived on the local AS specified.

Parameters

- `internal` — Configures the peer as internal.
- `external` — Configures the peer as external.
Other BGP-Related Commands

autonomous-system

**Syntax**

```
autonomous-system as-number
no autonomous-system
```

**Context**

`config>router`

**Description**

This command configures the autonomous system (AS) number for the router. A router can only belong to one AS. An AS number is a globally unique number with an AS. This number is used to exchange exterior routing information with neighboring ASs and as an identifier of the AS itself.

If the AS number is changed on a router with an active BGP instance, the new AS number is not used until the BGP instance is restarted either by administratively disabling/enabling (`shutdown/no shutdown`) the BGP instance or rebooting the system with the new configuration.

**Default**

No autonomous system number is defined.

**Parameters**

as-number — The autonomous system number expressed as a decimal integer.

**Values**

1 — 4294967295

mh-primary-interface

**Syntax**

```
mh-primary-interface interface-name
no mh-primary-interface
```

**Context**

`config>router`

**Description**

This command creates a loopback interface for the use in multihoming resilency. Once active this interface can be used to advertise reachability information to the rest of the network using the primary address which is backed up by the secondary.

This reachability for this address is advertised via IGPs and LDP protocols to allow the resolution of BGP routes advertised with this address.

The no form of the command disables this setting.

**Default**

`no mh-primary-interface`
Other BGP-Related Commands

mh-secondary-interface

Syntax  

```
mh-secondary-interface interface-name
no mh-secondary-interface
```

Context  

`config>router`

Description  

This command creates a loopback interface for the use in multihoming resiliency. This address is considered the secondary multihoming address and is only used to resolve routes advertised by the primary router in the event that router becomes unavailable. For this purpose, the Reachability for this address is advertised via IGP and LDP protocols to allow the resolution of BGP routes advertised with this address by the primary multihoming router.

The no form of the command disables this setting.

Default  

`no mh-secondary-interface`

address

Syntax  

```
address {ip-address/mask | ip-address netmask}
no address
```

Context  

`config>router>mh-primary-interface`

`config>router>mh-secondary-interface`

Description  

This command assigns an IP address, IP subnet, and broadcast address format to an IP interface. Only one IP address can be associated with an IP interface.

An IP address must be assigned to each IP interface for the interface to be active. An IP address and a mask combine to create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the router.

The local subnet that the address command defines must not be part of the services address space within the routing context by use of the config router service-prefix command. Once a portion of the address space is allocated as a service prefix, that portion is not available to IP interfaces for network core connectivity.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. Show commands display CIDR notation and are stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

The no form of the command removes the IP address assignment from the IP interface. Interface specific configurations for IGP protocols like OSPF are also removed. The no form of this command can only be performed when the IP interface is administratively shut down. Shutting down the IP interface will operationally stop any protocol interfaces or MPLS LSPs that explicitly reference that IP address. When a new IP address is defined, the IP interface can be administratively enabled (no shutdown), which reinitializes the protocol interfaces and MPLS LSPs associated with that IP interface.

If a new address is entered while another address is still active, the new address will be rejected.

Default  

`no address`
Parameters

- **ip-address** — The IP address of the IP interface. The ip-addr portion of the address command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

  **Values**

  - 1.0.0.0 — 223.255.255.255

  / — The forward slash is a parameter delimiter that separates the ip-addr portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the ipaddr, the “/,” and the mask-length parameter. If a forward slash does not immediately follow the ipaddr, a dotted decimal mask must follow the prefix.

- **mask-length** — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the ip-addr from the mask-length parameter. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. Allowed values are integers in the range 1 — 32. Note that a mask length of 32 is reserved for system IP addresses.

  **Values**

  - 1 — 3

- **mask** — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the ip-addr from a traditional dotted decimal mask. The mask parameter indicates the complete mask that will be used in a logical ‘AND’ function to derive the local subnet of the IP address. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

  **Values**

  - 128.0.0.0 — 255.255.255.255

- **net-mask** — The subnet mask in dotted decimal notation.

  **Values**

  - 0.0.0.0 — 223.255.255.255 (network bits all 1 and host bits all 0)

**description**

**Syntax**

```
    description description-string
    no description
```

**Context**

```
    config>router>mh-primary-interface
    config>router>mh-secondary-interface
```

**Description**

This command creates a text description stored in the configuration file for a configuration context.

The no form of the command removes the description string from the context.

**Default**

```
    no description
```

**Parameters**

- **description-string** — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
Other BGP-Related Commands

shutdown

Syntax  
shutdown  
no shutdown

Context  
config>router>mh-primary-interface  
config>router>mh-secondary-interface

Description  
The shutdown command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system generated configuration files.

The no form of the command puts an entity into the administratively enabled state.

Default  
no shutdown

hold-time

Syntax  
hold-time  
holdover-time

no hold-time

Context  
config>router>mh-secondary-interface

Description  
The optional hold-time parameter is only applicable for the secondary context and specifies how long label information learned about the secondary anycast address should be kept after that peer is declared down. This timer should be set to a value large enough for the remainder of the network to detect the failure and complete the reconvergence process.

The no form of the command resets the hold-time back to the default value.

Default  
no hold-time

Parameters  
holdover-time — (seconds) specifies the number of seconds the router should hold label information learned from the alternate router in its secondary label table. This is to allow the reset of the network to reconverge after a router failure before the anycast based label assignments are flushed from the forwarding plane.

Values  
0—65535

Default  
90
router-id

**Syntax**
- `router-id ip-address`
- `no router-id`

**Context**
`config>router`

**Description**
This command configures the router ID for the router instance.

The router ID is used by OSPF routing protocols in this instance of the routing table manager. IS-IS uses the router ID value as its system ID.

When configuring a new router ID, protocols are not automatically restarted with the new router ID. The next time a protocol is initialized, the new router ID is used. This can result in an interim period of time when different protocols use different router IDs.

To force the new router ID to be used, issue the `shutdown` and `no shutdown` commands for each protocol that uses the router ID, or restart the entire router.

The `no` form of the command reverts to the default value.

**Default**
The system uses the system interface address (which is also the loopback address).
If a system interface address is not configured, use the last 32 bits of the chassis MAC address.

**Parameters**
- `router-id` — The 32 bit router ID expressed in dotted decimal notation or as a decimal value.
Show Commands

**router**

**Syntax**
```
router [router-instance]
```

**Context**
```
show
```

**Description**
Displays router instance information.

**Parameters**

- `router-instance` — Specify either the router-name or service-id

**Values**
- `router-name`: Base, management
- `service-id`: 1 — 2147483647

**Default**
Base

**bgp**

**Syntax**
```
bgp
```

**Context**
```
show>router
```

**Description**
Enables the context to display BGP related information.

**auth-keychain**

**Syntax**
```
auth-keychain [keychain]
```

**Context**
```
show>router>bgp
show>router>bgp>group
```

**Description**
This command displays BGP sessions using particular authentication key-chain.

**Parameters**

- `keychain` — Specifies an existing keychain name.

**Sample Output**

```
*A:ALA-48# show router 2 bgp auth-keychain

Sessions using key chains

<table>
<thead>
<tr>
<th>Peer address</th>
<th>Group</th>
<th>Keychain name</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.1.3</td>
<td>1</td>
<td>eta_keychain1</td>
</tr>
<tr>
<td>30.1.0.2</td>
<td>1</td>
<td>eta_keychain1</td>
</tr>
</tbody>
</table>
```
Show Commands

*A:ALA-48#* 
*A:ALA-48(config-router)bgp#* show router bgp group "To_AS_10000"

BGP Group : To_AS_10000

Group Type       : No Type              State            : Up
Peer AS          : 10000                Local AS         : 200
Local Address    : n/a                  Loop Detect      : Ignore
Import Policy    : None Specified / Inherited
Hold Time        : 90                   Keep Alive       : 30
Cluster Id       : 0.0.0.100            Client Reflect   : Enabled
TTL Security     : Disabled             Min TTL Value    : n/a
Graceful Restart : Enabled              Stale Routes Time: 360
Auth key chain   : testname

List of Peers
- 10.0.0.8 :
  To_Router B - EBGP Peer

Peer Groups : 1

*A:ALA-48(config-router)bgp#*

*A:ALA-48(config-router)bgp#* show router bgp neighbor 10.0.0.8

BGP Neighbor

Peer  : 10.0.0.8
Group : To_AS_10000

Peer AS              : 10000            Peer Port            : 0
Peer Address         : 10.0.0.8
Local AS             : 200              Local Port           : 0
Local Address        : 0.0.0.0
Peer Type            : External
State                : Active           Last State           : Idle
Last Event           : stop
Last Error           : Cease
Local Family         : IPv4
Remote Family        : Unused
Hold Time            : 90               Keep Alive           : 30
Active Hold Time     : 0                Active Keep Alive    : 0
Cluster Id           : 0.0.0.100
Preference           : 99               Num of Flaps         : 0
Recd. Paths          : 0
IPv4 Recd. Prefixes  : 0                IPv4 Active Prefixes : 0
IPv4 Suppressed Prefixes : 0
VPN-IPv4 Suppr. Prefixes : 0
VPN-IPv4 Recd. Prefixes : 0
VPN-IPv4 Active Prefixes : 0
Mc IPv4 Recd. Prefixes : 0
Mc IPv4 Active Prefixes : 0
Mc IPv4 Suppr. Prefixes : 0
Input Queue          : 0                Output Queue         : 0
i/p Messages         : 0                o/p Messages         : 0
i/p Octets           : 0                o/p Octets           : 0
i/p Updates : 0          o/p Updates : 0
TTL Security : Disabled  Min TTL Value : n/a
Graceful Restart : Enabled Stale Routes Time : 360
Advertise Inactive : Disabled Peer Tracking : Disabled
Advertise Label : None
Auth key chain : testname
Local Capability : RouteRefresh MP-BGP
Remote Capability :
Import Policy : None Specified / Inherited
-------------------------------------------------------------------------------
Neighbors : 1
===============================================================================
*A:ALA-48>config>router>bgp#

*A:ALA-48>config>router>bgp# show router bgp auth-keychain testname
========================================================================= Sessions using key chain: keychain
========================================================================= Peer address Group Keychain name
------------------------------------------------------------------------- 10.0.0.8 To_AS_10000 testname
=========================================================================
*A:ALA-48>config>router>bgp#

damping

Syntax  damping [damp-type] [detail]
       damping [ip-prefix | prefix-length] [detail]

Context  show>router>bgp

Description This command displays BGP routes which have been dampened due to route flapping. This command can be entered with or without a route parameter.

When the keyword detail is included, more detailed information displays.

When only the command is entered (without any parameters included except detail), then all dampened routes are listed.

When a parameter is specified, then the matching route or routes are listed.

When a decayed, history, or suppressed keyword is specified, only those types of dampened routes are listed.

Parameters

   ip-prefix — Displays damping information for the specified IP prefix and length.

   Values  ipv4-prefix  a.b.c.d (host bits must be 0)
           ipv4-prefix-length  0 — 32

   damp-type — Specifies the type of damping to display.

   Values  decayed — Displays damping entries that are decayed but are not suppressed.
           history — Displays damping entries that are withdrawn but have history. suppressed — Displays damping entries suppressed because of route damping.
**Show Commands**

**detail** — Displays detailed information.

**Output Damping Output Fields** — The following table describes BGP damping output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>The local BGP Router ID</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured or inherited local AS for the specified peer group. If not configured, then it is the same value as the AS.</td>
</tr>
<tr>
<td>Network</td>
<td>Route IP prefix and mask length for the route.</td>
</tr>
<tr>
<td>Flag(s)</td>
<td>Legend:</td>
</tr>
<tr>
<td></td>
<td>Status codes: u- used, s-suppressed, h-history, d-decayed, *-valid. If a * is not present, then the status is invalid.</td>
</tr>
<tr>
<td></td>
<td>Origin codes: i-IGP, e-EGP, ?-incomplete, &gt;-best</td>
</tr>
<tr>
<td>From</td>
<td>The originator ID path attribute value.</td>
</tr>
<tr>
<td>Reuse time</td>
<td>The time when a suppressed route can be used again.</td>
</tr>
<tr>
<td>From</td>
<td>The originator ID path attribute value.</td>
</tr>
<tr>
<td>Reuse time</td>
<td>The time when a suppressed route can be used again.</td>
</tr>
<tr>
<td>AS Path</td>
<td>The BGP AS path for the route.</td>
</tr>
<tr>
<td>Peer</td>
<td>The router ID of the advertising router.</td>
</tr>
<tr>
<td>NextHop</td>
<td>BGP nexthop for the route.</td>
</tr>
<tr>
<td>Peer AS</td>
<td>The autonomous system number of the advertising router.</td>
</tr>
<tr>
<td>Peer Router-Id</td>
<td>The router ID of the advertising router.</td>
</tr>
<tr>
<td>Local Pref</td>
<td>BGP local preference path attribute for the route.</td>
</tr>
<tr>
<td>Age</td>
<td>The length of time in hour/minute/second (HH:MM:SS) format.</td>
</tr>
<tr>
<td>Last update</td>
<td>The time when BGP was updated last in day/hour/minute (DD:HH:MM) format.</td>
</tr>
<tr>
<td>FOM Present</td>
<td>The current Figure of Merit (FOM) value.</td>
</tr>
<tr>
<td>Number of Flaps</td>
<td>The number of route flaps in the neighbor connection.</td>
</tr>
<tr>
<td>Reuse time</td>
<td>The time when the route can be reused.</td>
</tr>
<tr>
<td>Path</td>
<td>The BGP AS path for the route.</td>
</tr>
<tr>
<td>Applied Policy</td>
<td>The applied route policy name.</td>
</tr>
</tbody>
</table>
### Sample Output

A:ALA-12# show router bgp damping

```
BGP Damped Routes
```

<table>
<thead>
<tr>
<th>Flag</th>
<th>Network</th>
<th>From</th>
<th>Reuse</th>
<th>AS-Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>ud*i</td>
<td>12.149.7.0/24</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.6.0/23</td>
<td>10.0.28.1</td>
<td>00h43m41s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.8.0/22</td>
<td>10.0.28.1</td>
<td>00h38m31s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.12.0/22</td>
<td>10.0.28.1</td>
<td>00h35m41s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.22.0/23</td>
<td>10.0.28.1</td>
<td>00h35m41s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.24.0/22</td>
<td>10.0.28.1</td>
<td>00h35m41s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.28.0/22</td>
<td>10.0.28.1</td>
<td>00h34m31s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.40.0/21</td>
<td>10.0.28.1</td>
<td>00h28m24s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>si</td>
<td>24.155.48.0/20</td>
<td>10.0.28.1</td>
<td>00h28m24s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>ud*i</td>
<td>61.8.140.0/24</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>ud*i</td>
<td>61.8.141.0/24</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>ud*i</td>
<td>61.9.0.0/18</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203 65001 19855 3356</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ud*i</td>
<td>62.213.184.0/23</td>
<td>10.0.28.1</td>
<td>00h00m00s</td>
<td>60203 65001 19855 3356</td>
</tr>
</tbody>
</table>

A:ALA-12#
A:ALA-12# show router bgp damping detail
-----------------------------------------------------------------------------------------------
BGP Router ID : 10.0.0.14         AS : 65206 Local AS : 65206
-----------------------------------------------------------------------------------------------
Legend -
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes  : i - IGP, e - EGP, ? - incomplete, - best
-----------------------------------------------------------------------------------------------
BGP Damped Routes
-----------------------------------------------------------------------------------------------
Network : 12.149.7.0/24
-----------------------------------------------------------------------------------------------
Network          : 12.149.7.0/24        Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
FOM Present      : 738                  FOM Last upd.    : 2039
Number of Flaps  : 2                    Flags            : ud*i
Path             : 60203 65001 19855 356 1239 22406
Applied Policy   : default-damping-profile
-----------------------------------------------------------------------------------------------
Network : 15.142.48.0/20
-----------------------------------------------------------------------------------------------
Network          : 15.142.48.0/20       Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
FOM Present      : 2031                 FOM Last upd.    : 2023
Number of Flaps  : 2                    Flags            : ud*i
Path             : 60203 65001 19855 356 3561 5551 1889
Applied Policy   : default-damping-profile
-----------------------------------------------------------------------------------------------
Network : 15.200.128.0/19
-----------------------------------------------------------------------------------------------
Network          : 15.200.128.0/19      Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
FOM Present      : 1018                 FOM Last upd.    : 2023
Number of Flaps  : 2                    Flags            : ud*i
Path             : 60203 65001 19855 1299 702 1889
Applied Policy   : default-damping-profile
-----------------------------------------------------------------------------------------------
Network : 15.203.192.0/18
-----------------------------------------------------------------------------------------------
Network          : 15.203.192.0/18     Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h00m00s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
FOM Present      : 1018                 FOM Last upd.    : 1024
Number of Flaps  : 1                    Flags            : ud*i
Path             : 60203 65001 19855 1299 702 1889
Applied Policy   : default-damping-profile
show router bgp damping 15.203.192.0/18 detail

Network : 15.203.192.0/18

Network          : 15.203.192.0/18       Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h29m22s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h01m28s            Last update      : 02d01h20m
FOM Present      : 2936                 FOM Last upd.    : 3001
Number of Flaps  : 3                    Flags            : si
Path             : 60203 65001 19855 3356  702   1889
Applied Policy   : default-damping-profile

Paths : 1

show router bgp damping suppressed detail

Network : 15.200.128.0/19

Network          : 15.200.128.0/19      Peer             : 10.0.28.1
NextHop          : 10.0.28.1            Reuse time       : 00h29m22s
Peer AS          : 60203                Peer Router-Id   : 32.32.27.203
Local Pref       : none
Age              : 00h01m28s            Last update      : 02d01h20m
FOM Present      : 2936                 FOM Last upd.    : 3001
Number of Flaps  : 3                    Flags            : si
Path             : 60203 65001 19855 3356  702   1889
Applied Policy   : default-damping-profile

Paths : 1
### Show Commands

<table>
<thead>
<tr>
<th>Age</th>
<th>Last update</th>
</tr>
</thead>
<tbody>
<tr>
<td>00h01m28s</td>
<td>02d01h20m</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FOM Present</th>
<th>FOM Last upd.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2936</td>
<td>3001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Flaps</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>si</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>60203 65001 19855 3356 702 1889</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applied Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-damping-profile</td>
</tr>
</tbody>
</table>

---

**Network**: 15.203.240.0/20

<table>
<thead>
<tr>
<th>Network</th>
<th>Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.203.240.0/20</td>
<td>10.0.28.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NextHop</th>
<th>Reuse time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.28.1</td>
<td>00h29m22s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peer AS</th>
<th>Peer Router-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>60203</td>
<td>32.32.27.203</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Pref</th>
<th>Last update</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>02d01h20m</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FOM Present</th>
<th>FOM Last upd.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2936</td>
<td>3001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Flaps</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>si</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>60203 65001 19855 3356 702 1889</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applied Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-damping-profile</td>
</tr>
</tbody>
</table>

---

**Network**: 15.206.0.0/17

<table>
<thead>
<tr>
<th>Network</th>
<th>Peer</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.206.0.0/17</td>
<td>10.0.28.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NextHop</th>
<th>Reuse time</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.28.1</td>
<td>00h29m22s</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Peer AS</th>
<th>Peer Router-Id</th>
</tr>
</thead>
<tbody>
<tr>
<td>60203</td>
<td>32.32.27.203</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Local Pref</th>
<th>Last update</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>02d01h20m</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FOM Present</th>
<th>FOM Last upd.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2936</td>
<td>3001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Flaps</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>si</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>60203 65001 19855 3356 702 1889</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Applied Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-damping-profile</td>
</tr>
</tbody>
</table>

---

A:ALA-12#

---

**group**

**Syntax**

```
group [name] [detail]
```

**Context**

```
show>router>bgp
```

**Description**

This command displays group information for a BGP peer group. This command can be entered with or without parameters.

When this command is entered without a group name, information about all peer groups displays.

When the command is issued with a specific group name, information only pertaining to that specific peer group displays.

The ‘State’ field displays the BGP group’s operational state. Valid states are:

- **Up** — BGP global process is configured and running.
- **Down** — BGP global process is administratively shutdown and not running.
- **Disabled** — BGP global process is operationally disabled. The process must be restarted by the operator.

**Parameters**

- **name** — Displays information for the BGP group specified.
- **detail** — Displays detailed information.

---
**Output Standard and Detailed Group Output** — The following table describes the standard and detailed command output fields for a BGP group.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>Displays the BGP group name.</td>
</tr>
<tr>
<td>Group Type</td>
<td>No Type — Peer type not configured.</td>
</tr>
<tr>
<td></td>
<td>External — Peer type configured as external BGP peers.</td>
</tr>
<tr>
<td></td>
<td>Internal — Peer type configured as internal BGP peers.</td>
</tr>
<tr>
<td>State</td>
<td>Disabled — The BGP peer group has been operationally disabled.</td>
</tr>
<tr>
<td></td>
<td>Down — The BGP peer group is operationally inactive.</td>
</tr>
<tr>
<td></td>
<td>Up — The BGP peer group is operationally active.</td>
</tr>
<tr>
<td>Peer AS</td>
<td>The configured or inherited peer AS for the specified peer group.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured or inherited local AS for the specified peer group.</td>
</tr>
<tr>
<td>Local Address</td>
<td>The configured or inherited local address for originating peering for the specified peer group.</td>
</tr>
<tr>
<td>Loop Detect</td>
<td>The configured or inherited loop detect setting for the specified peer group.</td>
</tr>
<tr>
<td>Connect Retry</td>
<td>The configured or inherited connect retry timer value.</td>
</tr>
<tr>
<td>Authentication</td>
<td>None — No authentication is configured.</td>
</tr>
<tr>
<td></td>
<td>MD5 — MD5 authentication is configured.</td>
</tr>
<tr>
<td>Bfd</td>
<td>Yes — BFD is enabled.</td>
</tr>
<tr>
<td></td>
<td>No — BFD is disabled.</td>
</tr>
<tr>
<td>Local Pref</td>
<td>The configured or inherited local preference value.</td>
</tr>
<tr>
<td>MED Out</td>
<td>The configured or inherited MED value assigned to advertised routes without a MED attribute.</td>
</tr>
<tr>
<td>Min Route Advt.</td>
<td>The minimum amount of time that must pass between route updates for the same IP prefix.</td>
</tr>
<tr>
<td>Min AS Originate</td>
<td>The minimum amount of time that must pass between updates for a route originated by the local router.</td>
</tr>
<tr>
<td>Multihop</td>
<td>The maximum number of router hops a BGP connection can traverse.</td>
</tr>
<tr>
<td>Prefix Limit</td>
<td>No Limit — No route limit assigned to the BGP peer group.</td>
</tr>
<tr>
<td></td>
<td>1 — 4294967295 — The maximum number of routes BGP can learn from a peer.</td>
</tr>
</tbody>
</table>
### Show Commands

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive</td>
<td>Disabled – BGP attempts to establish a BGP connection with neighbor in the specified peer group.</td>
</tr>
<tr>
<td></td>
<td>Enabled – BGP will not actively attempt to establish a BGP connection with neighbor in the specified peer group.</td>
</tr>
<tr>
<td>Next Hop Self</td>
<td>Disabled – BGP is not configured to send only its own IP address as the BGP nexthop in route updates to neighbors in the peer group.</td>
</tr>
<tr>
<td></td>
<td>Enabled – BGP sends only its own IP address as the BGP nexthop in route updates to neighbors in the specified peer group.</td>
</tr>
<tr>
<td>Aggregator ID 0</td>
<td>Disabled – BGP is not configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates sent to the neighbor in the peer group.</td>
</tr>
<tr>
<td></td>
<td>Enabled – BGP is configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates sent to the neighbor in the peer group.</td>
</tr>
<tr>
<td>Remove Private</td>
<td>Disabled – BGP will not remove all private AS numbers from the AS path attribute in updates sent to the neighbor in the peer group.</td>
</tr>
<tr>
<td></td>
<td>Enabled – BGP removes all private AS numbers from the AS path attribute in updates sent to the neighbor in the peer group.</td>
</tr>
<tr>
<td>Damping</td>
<td>Disabled – The peer group is configured not to dampen route flaps.</td>
</tr>
<tr>
<td></td>
<td>Enabled – The peer group is configured to dampen route flaps.</td>
</tr>
<tr>
<td>Export Policy</td>
<td>The configured export policies for the peer group.</td>
</tr>
<tr>
<td>Import Policy</td>
<td>The configured import policies for the peer group.</td>
</tr>
<tr>
<td>Hold Time</td>
<td>The configured hold time setting.</td>
</tr>
<tr>
<td>Keep Alive</td>
<td>The configured keepalive setting.</td>
</tr>
<tr>
<td>Cluster Id</td>
<td>The configured route reflector cluster ID.</td>
</tr>
<tr>
<td></td>
<td>None – No cluster ID has been configured</td>
</tr>
<tr>
<td>Client Reflect</td>
<td>Disabled – The BGP route reflector will not reflect routes to this neighbor.</td>
</tr>
<tr>
<td></td>
<td>Enabled – The BGP route reflector is configured to reflect routes to this neighbor.</td>
</tr>
<tr>
<td>NLRI</td>
<td>The type of NLRI information that the specified peer group can accept.</td>
</tr>
<tr>
<td></td>
<td>Unicast – IPv4 unicast routing information can be carried.</td>
</tr>
<tr>
<td>Preference</td>
<td>The configured route preference value for the peer group.</td>
</tr>
</tbody>
</table>
**Sample Output**

A:ALA-12# ```show router bgp group```

```
BGP Groups
-------------------------------------------------------------------------------
Group            : To_AS_40000
-------------------------------------------------------------------------------
Description      : Not Available
Group Type       : No Type              State            : Up
Peer AS          : 40000                Local AS         : 65206
Local Address    : n/a                  Loop Detect      : Ignore
Export Policy    : direct2bgp
Hold Time        : 90                   Keep Alive       : 30
Cluster Id       : None                 Client Reflect   : Enabled
NLRI             : Unicast              Preference       : 170
List of Peers
- 10.0.0.1       : To_Jukebox
- 10.0.0.12      : Not Available
- 10.0.0.13      : Not Available
- 10.0.0.14      : To_SR1
- 10.0.0.15      : To_H-215
Total Peers      : 5                    Established      : 2
```

A:ALA-12#

**Sample Detailed Output**

A:ALA-12# ```show router bgp group detail```

```
BGP Groups (detail)
-------------------------------------------------------------------------------
Group            : To_AS_40000
-------------------------------------------------------------------------------
Description      : Not Available
Group Type       : No Type              State            : Up
Peer AS          : 40000                Local AS         : 65206
Local Address    : n/a                  Loop Detect      : Ignore
Connect Retry    : 20                   Authentication   : None
Local Pref       : 100                  MED Out          : 0
Multihop         : 0 (Default)         Min Route Advt. : 30
Min Route Advt.  : 30                   Min AS Originate : 15
Prefix Limit     : No Limit            Passive          : Disabled
Next Hop Self    : Disabled            Aggregator ID 0  : Disabled
Remove Private   : Disabled            Damping          : Disabled
Export Policy    : direct2bgp
```

---

**Label** | **Description (Continued)**
---|---
List of Peers | A list of BGP peers configured under the peer group.
Total Peers | The total number of peers configured under the peer group.
Established | The total number of peers that are in an established state.
Show Commands

Hold Time : 90  Keep Alive : 30
Cluster Id : None  Client Reflect : Enabled
NLRI : Unicast  Preference : 170

List of Peers
- 10.0.0.1 : To_Jukebox
- 10.0.0.12 : Not Available
- 10.0.0.13 : Not Available
- 10.0.0.14 : To_SR1
- 10.0.0.15 : To_H-215

Total Peers : 5  Established : 2

A:ALA-12#

A:SetupCLI>show>router:bgp group

BGP Group

Group : bgp_group_1 34567890123456789012

Description : Testing the length of the group value for the DESCRIPTION parameter of BGP
Group Type : No Type  State : Up
Peer AS : n/a  Local AS : 100
Local Address : n/a  Loop Detect : Ignore
Import Policy : test i1
               : test i2
               : test i3
               : test i4
               : test i5 890123456789012345678901
Export Policy : test e1
               : test e2
               : test e3
               : test e4
               : test e5 890123456789012345678901
Hold Time : 120  Keep Alive : 30
Cluster Id : None  Client Reflect : Enabled
NLRI : Unicast  Preference : 101
TTL Security : Disabled  Min TTL Value : n/a
Graceful Restart : Disabled  Stale Routes Time: n/a
Auth key chain : n/a  Bfd Enabled : Yes

List of Peers
- 3.3.3.3 :
  Testing the length of the neighbor value for the DESCRIPTION parameter of BGP

Total Peers : 1  Established : 0

Peer Groups : 1

A:SetupCLI>show>router:bgp#
neighbor

Syntax

neighbor [ip-address [detail]]
neighbor [as-number [detail]]
neighbor ip-address [family [type mvpn-type]] filter1 [brief]
neighbor ip-address [family] filter2
neighbor as-number [family] filter2
neighbor ip-address orf [filter3]
neighbor ip-address graceful-restart

Context

show>router>bgp

Description

This command displays BGP neighbor information. This command can be entered with or without any parameters.

When this command is issued without any parameters, information about all BGP peers displays.

When the command is issued with a specific IP address or ASN, information regarding only that specific peer or peers with the same AS displays.

When either received-routes or advertised-routes is specified, then the routes received from or sent to the specified peer is listed (see second output example).

Note: This information is not available by SNMP.

When either history or suppressed is specified, then the routes learned from those peers that either have a history or are suppressed (respectively) are listed.

The ‘State’ field displays the BGP peer’s protocol state. In additional to the standard protocol states, this field can also display the ‘Disabled’ operational state which indicates the peer is operationally disabled and must be restarted by the operator.

Parameters

ip-address — Display information for the specified IP address.

Values

ipv4-address: a.b.c.d (host bits must be 0)
interface: 32 characters maximum, mandatory for link local addresses.

as-number — Display information for the specified AS number.

Values

1 — 65535

family — Specify the type of routing information to be distributed by this peer group.

Values

ipv4 — Displays only those BGP peers that have the IPv4 family enable and not those capable of exchanging IP-VPN routes.
vpn-ipv4 — Displays the content of the multicast routing table.
mcast-ipv4 — Displays the BGP peers that are mcast-ipv4 capable.

filter1 — Display information for the specified IP address.

Values

received-routes — Displays the number of routes received from this peer.
advertised-routes — Displays the number of routes advertised by this peer.
history — Displays statistics for dampened routes.
suppressed — Displays the number of paths from this peer that have been suppressed by damping.
detail — Displays detailed information pertaining to filter1.
Show Commands

*filter2* — Display information for the specified AS number.

**Values**
- **history** — Display statistics for dampened routes.
- **suppressed** — Display the number of paths from this peer that have been suppressed by damping.
- **detail** — Displays detailed information pertaining to *filter2*

*filter3* — Displays path information for the specified IP address.

**Values**
- **send** — Displays the number of paths sent to this peer.
- **receive** — Displays the number of paths received from this peer.

**brief** — Displays information in a brief format. This parameter is only supported with received-routes and advertised-routes.

*orf* — Displays outbound route filtering for the BGP instance. ORF (Outbound Route Filtering) is used to inform a neighbor of targets (using target-list) that it is willing to receive. This mechanism helps lessen the update exchanges between neighbors and saves CPU cycles to process routes that could have been received from the neighbor only to be dropped/ignored.

*graceful-restart* — Displays neighbors configured for graceful restart.

**Output**

### Standard and Detailed Neighbor

The following table describes the standard and detailed command output fields for a BGP neighbor.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer</td>
<td>The IP address of the configured BGP peer.</td>
</tr>
<tr>
<td>Group</td>
<td>The BGP peer group to which this peer is assigned.</td>
</tr>
<tr>
<td>Peer AS</td>
<td>The configured or inherited peer AS for the peer group.</td>
</tr>
<tr>
<td>Peer Address</td>
<td>The configured address for the BGP peer.</td>
</tr>
<tr>
<td>Peer Port</td>
<td>The TCP port number used on the far-end system.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured or inherited local AS for the peer group.</td>
</tr>
<tr>
<td>Local Address</td>
<td>The configured or inherited local address for originating peering for the peer group.</td>
</tr>
<tr>
<td>Local Port</td>
<td>The TCP port number used on the local system.</td>
</tr>
<tr>
<td>Peer Type</td>
<td><strong>External</strong> — Peer type configured as external BGP peers.</td>
</tr>
<tr>
<td></td>
<td><strong>Internal</strong> — Peer type configured as internal BGP peers.</td>
</tr>
<tr>
<td>Bfd</td>
<td><strong>Yes</strong> — BFD is enabled.</td>
</tr>
<tr>
<td></td>
<td><strong>No</strong> — BFD is disabled.</td>
</tr>
<tr>
<td>State</td>
<td><strong>Idle</strong> — The BGP peer is not accepting connections.</td>
</tr>
<tr>
<td></td>
<td><strong>Active</strong> — BGP is listening for and accepting TCP connections from this peer.</td>
</tr>
<tr>
<td>Label</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connect</td>
<td>BGP is attempting to establish a TCP connection from this peer.</td>
</tr>
<tr>
<td>Open Sent</td>
<td>BGP has sent an OPEN message to the peer and is waiting for a reply.</td>
</tr>
<tr>
<td>Open Confirm</td>
<td>BGP has received a valid OPEN message from the peer and is awaiting KEEPALIVE or NOTIFICATION.</td>
</tr>
<tr>
<td>Established</td>
<td>BGP has successfully established a peering and is exchanging routing info.</td>
</tr>
<tr>
<td>Idle</td>
<td>The BGP peer is not accepting connections.</td>
</tr>
<tr>
<td>Active</td>
<td>BGP is listening for and accepting TCP connections from this peer.</td>
</tr>
<tr>
<td>Connect</td>
<td>BGP is attempting to establish a TCP connection from this peer.</td>
</tr>
<tr>
<td>Open Sent</td>
<td>BGP has sent an OPEN message to the peer and is waiting for a reply.</td>
</tr>
<tr>
<td>Open Confirm</td>
<td>BGP has received a valid OPEN message from the peer and is awaiting KEEPALIVE or NOTIFICATION.</td>
</tr>
<tr>
<td>Last State</td>
<td>start — BGP has initialized the BGP neighbor.</td>
</tr>
<tr>
<td></td>
<td>stop — BGP has disabled the BGP neighbor.</td>
</tr>
<tr>
<td></td>
<td>open — BGP transport connection opened.</td>
</tr>
<tr>
<td></td>
<td>close — BGP transport connection closed.</td>
</tr>
<tr>
<td></td>
<td>openFail — BGP transport connection failed to open.</td>
</tr>
<tr>
<td></td>
<td>error — BGP transport connection error.</td>
</tr>
<tr>
<td></td>
<td>connectRetry — Connect retry timer expired.</td>
</tr>
<tr>
<td></td>
<td>holdTime — Hold time timer expired.</td>
</tr>
<tr>
<td></td>
<td>keepAlive — Keepalive timer expired.</td>
</tr>
<tr>
<td></td>
<td>recvOpen — Receive an OPEN message.</td>
</tr>
<tr>
<td></td>
<td>revKeepalive — Receive a KEEPALIVE message.</td>
</tr>
<tr>
<td></td>
<td>recvUpdate — Receive an UPDATE message.</td>
</tr>
<tr>
<td></td>
<td>recvNotify — Receive a NOTIFICATION message.</td>
</tr>
<tr>
<td></td>
<td>None — No events have occurred.</td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Error</td>
<td>Displays the last BGP error and subcode to occur on the BGP neighbor.</td>
</tr>
<tr>
<td>Connect Retry</td>
<td>The configured or inherited connect retry timer value.</td>
</tr>
<tr>
<td>Local Pref.</td>
<td>The configured or inherited local preference value.</td>
</tr>
<tr>
<td>Min Route Advt.</td>
<td>The minimum amount of time that must pass between route updates for the same IP prefix.</td>
</tr>
<tr>
<td>Min AS Originated</td>
<td>The minimum amount of time that must pass between updates for a route originated by the local router.</td>
</tr>
<tr>
<td>Multihop</td>
<td>The maximum number of router hops a BGP connection can traverse.</td>
</tr>
<tr>
<td>Damping</td>
<td>Disabled — BGP neighbor is configured not to dampen route flaps.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP neighbor is configured to dampen route flaps.</td>
</tr>
<tr>
<td>Loop Detect</td>
<td>Ignore — The BGP neighbor is configured to ignore routes with an AS loop.</td>
</tr>
<tr>
<td></td>
<td>Drop — The BGP neighbor is configured to drop the BGP peering if an AS loop is detected.</td>
</tr>
<tr>
<td></td>
<td>Off — AS loop detection is disabled for the neighbor.</td>
</tr>
<tr>
<td>MED Out</td>
<td>The configured or inherited MED value assigned to advertised routes without a MED attribute.</td>
</tr>
<tr>
<td>Authentication</td>
<td>None — No authentication is configured.</td>
</tr>
<tr>
<td></td>
<td>MD5 — MD5 authentication is configured.</td>
</tr>
<tr>
<td>Next Hop Self</td>
<td>Disabled — BGP is not configured to send only its own IP address as the BGP nexthop in route updates to the specified neighbor.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP will send only its own IP address as the BGP nexthop in route updates to the neighbor.</td>
</tr>
<tr>
<td>AggregatorID Zero</td>
<td>Disabled — The BGP Neighbor is not configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates.</td>
</tr>
<tr>
<td></td>
<td>Enabled — The BGP Neighbor is configured to set the aggregator ID to 0.0.0.0 in all originated route aggregates.</td>
</tr>
<tr>
<td>Remove Private</td>
<td>Disabled — BGP will not remove all private AS numbers from the AS path attribute, in updates sent to the specified neighbor.</td>
</tr>
<tr>
<td></td>
<td>Enabled — BGP will remove all private AS numbers from the AS path attribute, in updates sent to the specified neighbor.</td>
</tr>
</tbody>
</table>
### Label | Description (Continued)
--- | ---
Passive | **Disabled** — BGP will actively attempt to establish a BGP connection with the specified neighbor.
| **Enabled** — BGP will not actively attempt to establish a BGP connection with the specified neighbor.
Prefix Limit | **No Limit** — No route limit assigned to the BGP peer group.
| 1 — 4294967295 — The maximum number of routes BGP can learn from a peer.
Hold Time | The configured hold time setting.
Keep Alive | The configured keepalive setting.
Active Hold Time | The negotiated hold time, if the BGP neighbor is in an established state.
Active Keep Alive | The negotiated keepalive time, if the BGP neighbor is in an established state.
Cluster Id | The configured route reflector cluster ID.
| **None** — No cluster ID has been configured.
Client Reflect | **Disabled** — The BGP route reflector is configured not to reflect routes to this neighbor.
| **Enabled** — The BGP route reflector is configured to reflect routes to this neighbor.
Preference | The configured route preference value for the peer group.
Num of Flaps | The number of route flaps in the neighbor connection.
Recd. Prefixes | The number of routes received from the BGP neighbor.
Active Prefixes | The number of routes received from the BGP neighbor and active in the forwarding table.
Recd. Paths | The number of unique sets of path attributes received from the BGP neighbor.
Suppressed Paths | The number of unique sets of path attributes received from the BGP neighbor and suppressed due to route damping.
Input Queue | The number of BGP messages to be processed.
Output Queue | The number of BGP messages to be transmitted.
i/p Messages | Total number of packets received from the BGP neighbor.
o/p Messages | Total number of packets sent to the BGP neighbor.
**Show Commands**

**Label** | **Description (Continued)**
--- | ---
i/p Octets | Total number of octets received from the BGP neighbor.
o/p Octets | Total number of octets sent to the BGP neighbor.
Export Policy | The configured export policies for the peer group.
Import Policy | The configured import policies for the peer group.

**Sample Output**

```
A:ALA-40# show router bgp neighbor

BGP Neighbor

Peer : 10.0.0.5     Group : headquarters1
Peer AS : 300       Peer Port : 0
Peer Address : 10.0.0.5
Local AS : 200      Local Port : 0
Local Address : 10.0.0.104
Peer Type : External
State : Active      Last State : Idle
Last Event : stop
Last Error : Cease
Local Family : IPv4  Remote Family : Unused
Hold Time : 90      Keep Alive : 30
Active Hold Time : 0     Active Keep Alive: 0
Cluster Id : 0.0.0.100
Preference : 170     Num of Flaps : 0
Recd. Prefixes : 0   Active Prefixes : 0
Recd. Paths : 0      Suppressed Paths : 0
Input Queue : 0      Output Queue : 0
i/p Messages : 0     o/p Messages : 0
i/p Octets : 0       o/p Octets : 0
i/p Updates : 0      o/p Updates : 0
TTL Security : Enabled  Min TTL Value : 255
Graceful Restart : Disabled  Stale Routes Time: n/a
Local Capability : RouteRefresh MP-BGP
Remote Capability:
Import Policy : None Specified / Inherited
Export Policy : None Specified / Inherited

Peer : 10.0.0.91     Group : Santa Clara
Peer AS : 100       Peer Port : 0
Peer Address : 10.0.0.91
Local AS : 200      Local Port : 0
Local Address : 10.0.0.103
Peer Type : External
State : Connect     Last State : Active
Last Event : openFail
Last Error : Cease
Local Family : IPv4  Remote Family : Unused
Hold Time : 90      Keep Alive : 30
Active Hold Time : 0     Active Keep Alive: 0
```
Cluster Id       : 0.0.0.100
Preference       : 170                  Num of Flaps     : 0
Recd. Prefixes   : 0                    Active Prefixes  : 0
Recd. Paths      : 0                    Suppressed Paths : 0
Input Queue      : 0                    Output Queue     : 0
i/p Messages     : 0                    o/p Messages     : 1
i/p Octets       : 0                    o/p Octets       : 0
i/p Updates      : 0                    o/p Updates       : 0
TTL Security     : Disabled             Min TTL Value    : n/a
Graceful Restart : Disabled             Stale Routes Time: n/a
Local Capability : RouteRefresh MP-BGP
Remote Capability:
Import Policy    : None Specified / Inherited
Export Policy    : None Specified / Inherited

-------------------------------------------------------------------------------
A:ALA-48#
A:ALA-48# show router 2 bgp neighbor 10.20.1.3
===============================================================================
BGP Neighbor
===============================================================================
Peer  : 10.20.1.3
Group : 1
-------------------------------------------------------------------------------
Peer AS              : 100              Peer Port            : 49725
Peer Address         : 10.20.1.3
Local AS             : 100              Local Port           : 179
Local Address        : 10.20.1.2
Peer Type            : Internal
State                : Established      Last State           : Established
Last Event           : recvKeepAlive
Last Error           : Cease
Local Family         : IPv4
Remote Family        : IPv4
Hold Time            : 3                Keep Alive           : 1
Active Hold Time     : 3                Active Keep Alive   : 1
Cluster Id           : None
Preference           : 170              Num of Flaps         : 0
Recd. Paths          : 11               IPv4 Active Prefixes : 10
IPv4 Recd. Prefixes  : 0                    VPN-IPv4 Suppr. Pfxs : 0
IPv4 Suppressed Pfxs : 0                    VPN-IPv4 Active Pfxs : 0
Mc IPv4 Recd. Pfxs   : 0                    Mc IPv4 Active Pfxs : 0
Mc IPv4 Suppr. Pfxs  : 0
Input Queue          : 0                    Output Queue         : 0
i/p Messages         : 471              o/p Messages         : 473
i/p Octets           : 3241             o/p Octets           : 3241
i/p Updates          : 4                    o/p Updates          : 4
TTL Security         : Disabled             Min TTL Value       : n/a
Advertise Inactive   : Disabled             Peer Tracking       : Disabled
Advertise Label      : None
Auth key chain       : eta_keychain1
Local Capability     : RouteRefresh MP-BGP
Remote Capability    : RouteRefresh MP-BGP
Import Policy        : None Specified / Inherited
Export Policy        : static2bgp
-------------------------------------------------------------------------------
Neighbors : 1
A:ALA-48#

A:ALA-12# show router bgp neighbor 10.0.0.11 orf

BGP Neighbor 10.0.0.11 ORF

Send List (Automatic)

```
target:65535:10
target:65535:20
```

A:ALA-12

A:ALA-22 show router bgp neighbor 10.0.0.1 orf

BGP Neighbor 10.0.0.1 ORF

Receive List

```
target:65535:10
target:65535:20
```

A:ALA-22

**Sample Detailed Output**

A:ALA-12# show router bgp neighbor detail

BGP Neighbor (detail)

```
Peer : 10.0.0.15         Group : To_AS_40000
-------------------------------------------------------------------------------
Peer AS          : 65205                Peer Port        : 0
Peer Address     : 10.0.0.15
Local AS         : 65206                Local Port       : 0
Local Address    : 10.0.0.16
Peer Type        : External
State            : Active               Last State       : Connect
Last Event       : openFail
Last Error       : Hold Timer Expire
Connect Retry    : 20                   Local Pref.      : 100
Min Route Advts. : 30                   Min AS Orig.     : 15
Damping          : Disabled             Loop Detect      : Ignore
MED Out          : No MED Out           Authentication   : None
Next Hop Self    : Disabled             AggregatorID Zero: Disabled
Remove Private   : Disabled             Passive          : Disabled
Prefix Limit     : No Limit
Hold Time        : 90                   Keep Alive       : 30
Active Hold Time : 0                    Active Keep Alive: 0
Cluster Id       : None                 Client Reflect   : Enabled
Preference       : 170                  Num of Flaps     : 0
Recd. Prefixes   : 0                    Active Prefixes  : 0
Recd. Paths      : 0                    Suppressed Paths : 0
Input Queue      : 0                    Output Queue     : 0
i/p Messages     : 0                    o/p Messages     : 0
```
A:ALA-12#

*A:SetupCLI>show>router:bgp# neighbor

BGP Neighbor

Peer  : 3.3.3.3
Group : bgp_group_1 34567890123456789012

Peer AS              : 20               Peer Port            : 0
Peer Address         : 3.3.3.3
Local AS             : 100              Local Port           : 0
Local Address        : 0.0.0.0
Peer Type            : Internal
State                : Active           Last State           : Idle
Last Event           : stop
Last Error           : Cease
Local Family         : IPv4
Remote Family        : Unused
Hold Time            : 10               Keep Alive           : 30
Active Hold Time     : 0                Active Keep Alive    : 0
Cluster Id           : 2.2.3.4
Preference           : 101              Num of Flaps         : 0
Recd. Paths          : 0
IPv4 Recd. Prefixes  : 0                IPv4 Active Prefixes : 0
IPv4 Suppressed Pfxs : 0                VPN-IPv4 Suppr. Pfxs : 0
VPN-IPv4 Recd. Pfxs  : 0                VPN-IPv4 Active Pfxs : 0
Mc IPv4 Recd. Pfxs.  : 0                Mc IPv4 Active Pfxs. : 0
Mc IPv4 Suppr. Pfxs  : 0
Input Queue          : 0                Output Queue         : 0
i/p Messages         : 0                o/p Messages         : 0
i/p Octets           : 0                o/p Octets           : 0
i/p Updates          : 0                o/p Updates          : 0
TTL Security         : Disabled         Min TTL Value        : n/a
Graceful Restart     : Enabled          Stale Routes Time    : 360
Advertise Inactive   : Disabled         Peer Tracking        : Enabled
Advertise Label      : None             Bfd Enabled     : Yes
Auth key chain       : n/a
Local Capability     : RouteRefresh MP-BGP
Remote Capability    :
Import Policy        :
: test i1
: test i2
: test i3
: test i4
: test i5 890123456789012345678901
Export Policy        :
: test e1
: test e2
: test e3
: test e4
: test e5 890123456789012345678901

Neighbors : 1

------------------------------------------------------------------------------------------------------------------------------------------------------
Advertised and Received Routes Output — The following table describes the command output for both the standard and detailed information for a neighbor.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured local AS setting. If not configured, then it is the same value as the AS.</td>
</tr>
<tr>
<td>Flag</td>
<td>u — used</td>
</tr>
<tr>
<td></td>
<td>s — suppressed</td>
</tr>
<tr>
<td></td>
<td>h — history</td>
</tr>
<tr>
<td></td>
<td>d — decayed</td>
</tr>
<tr>
<td></td>
<td>* — valid</td>
</tr>
<tr>
<td></td>
<td>i — igp</td>
</tr>
<tr>
<td></td>
<td>e — egp</td>
</tr>
<tr>
<td></td>
<td>? — incomplete</td>
</tr>
<tr>
<td></td>
<td>&gt; — best</td>
</tr>
<tr>
<td>Network</td>
<td>Route IP prefix and mask length for the route.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>BGP nexthop for the route.</td>
</tr>
<tr>
<td>LocalPref</td>
<td>BGP local preference path attribute for the route.</td>
</tr>
<tr>
<td>MED</td>
<td>BGP Multi-Exit Discriminator (MED) path attribute for the route.</td>
</tr>
<tr>
<td>AS Path</td>
<td>The BGP AS path for the route.</td>
</tr>
</tbody>
</table>

Sample Output

A:ALA-12# show router bgp neighbor 10.0.0.16 received-routes
===============================================================================
BGP Router ID : 10.0.0.16         AS : 65206   Local AS : 65206
===============================================================================
Legend -
Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes : i - IGP, e - EGP, ? - incomplete, > - best
===============================================================================
BGP Neighbor
Flag  Network            Nexthop         LocalPref  MED        As-Path
-------------------------------------------------------------------------------
?     10.0.0.16/32       10.0.0.16       100        none       No As-Path
?     10.0.6.0/24        10.0.0.16       100        none       No As-Path
?     10.0.8.0/24        10.0.0.16       100        none       No As-Path
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Next Hop</th>
<th>MED</th>
<th>Local Preference</th>
<th>AS Path</th>
<th>Origin</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.12.0/24</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
<td></td>
</tr>
<tr>
<td>10.0.13.0/24</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
<td></td>
</tr>
<tr>
<td>10.0.204.0/24</td>
<td>10.0.0.16</td>
<td>100</td>
<td>none</td>
<td>No As-Path</td>
<td></td>
</tr>
</tbody>
</table>

---

**A: core_east# show router bgp neighbor 10.193.0.10 graceful-restart**

---

**BGP Neighbor 10.193.0.10 Graceful Restart**

Graceful Restart locally configured for peer: Enabled
Peer's Graceful Restart feature: Enabled
NLRI(s) that peer supports restart for: IPv4-Unicast IPv4-MPLS IPv4-VPN
NLRI(s) that peer saved forwarding for: IPv4-Unicast IPv4-MPLS IPv4-VPN
NLRI(s) that restart is negotiated for: None
NLRI(s) of received end-of-rib markers: IPv4-Unicast
NLRI(s) of all end-of-rib markers sent: IPv4-Unicast
Restart time locally configured for peer: 120 seconds
Restart time requested by the peer: 390 seconds
Time stale routes from peer are kept for: 360 seconds
Graceful restart status on the peer: Not currently being helped
Number of Restarts: 328
Last Restart at: 08/20/2006 12:22:06

---

**next-hop**

**Syntax**

`next-hop [family] [ip-address] [detail]`

**Context**

`show>router>bgp`

**Description**

Displays BGP next-hop information.

**Parameters**

- **family** — Specify the type of routing information to be distributed by the BGP instance.
  - **Values**
    - `ipv4` — Displays only those BGP peers that have the IPv4 family enable and not those capable of exchanging IP-VPN routes.
    - `vpn-ipv4` — Displays the BGP peers that are IP-VPN capable.
    - `mcast-ipv4` — Displays the BGP peers that are mcast-ipv4 capable.
  - **Values**
    - `ip-address` — Displays the next hop information for the specified IP address.
      - **Values**
        - `ipv4-address: a.b.c.d (host bits must be 0)`
  - **detail** — Display the longer, more detailed version of the output.

**Output**

Show Next-Hop Output — The following table describes the command output fields for a BGP next hop.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
</tbody>
</table>
### Local AS
The configured local AS setting. If not configured, then the value is the same as the AS.

### Next Hop
The next-hop address.

### Resolving Prefix
Displays the prefix of the best next hop.

### Owner
Displays the routing protocol used to derive the best next hop.

### Preference
Displays the BGP preference attribute for the routes.

### Reference Count
Displays the number of routes using the resolving prefix.

### Resolved Next Hop
The IP address of the next hop.

#### Sample Output

*A:Dut-C# show router bgp next-hop

<table>
<thead>
<tr>
<th>Next Hop</th>
<th>Resolving Prefix</th>
<th>Owner</th>
<th>Preference</th>
<th>Reference Count</th>
<th>Resolved Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.20.1.1</td>
<td>10.20.1.1/32</td>
<td>RSVP</td>
<td>1000</td>
<td>2</td>
<td>10.20.1.1/32</td>
</tr>
<tr>
<td>10.10.2.1</td>
<td>10.20.1.2/32</td>
<td>RSVP</td>
<td>1000</td>
<td>2</td>
<td>10.20.1.2/32</td>
</tr>
<tr>
<td>10.20.1.4</td>
<td>10.20.1.4/32</td>
<td>RSVP</td>
<td>1000</td>
<td>2</td>
<td>10.20.1.4/32</td>
</tr>
</tbody>
</table>

Next Hops : 3

A:ALA-49> show router bgp# next-hop 10.10.10.104

<table>
<thead>
<tr>
<th>Next Hop</th>
<th>Resolving Prefix</th>
<th>Owner</th>
<th>Preference</th>
<th>Reference Count</th>
<th>Resolved Next Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.104</td>
<td>10.10.10.104</td>
<td>AS:200</td>
<td></td>
<td></td>
<td>10.10.10.104</td>
</tr>
</tbody>
</table>

A:ALA-49> show router bgp# next-hop 10.10.10.104
paths

Syntax
paths

Context
show>router:bgp

Description
This command displays a summary of BGP path attributes.

Output
Show Path Output — The following table describes the command output fields for a BGP path.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured local AS setting. If not configured, then the value is the same as the AS.</td>
</tr>
<tr>
<td>Path</td>
<td>The AS path attribute.</td>
</tr>
<tr>
<td>Origin</td>
<td>EGP — The NLRI is learned by an EGP protocol.</td>
</tr>
<tr>
<td></td>
<td>IGP — The NLRI is interior to the originating AS.</td>
</tr>
<tr>
<td></td>
<td>INCOMPLETE — NLRI was learned another way.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The advertised BGP nexthop.</td>
</tr>
<tr>
<td>MED</td>
<td>The Multi-Exit Discriminator value.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>The local preference value. This value is used if the BGP route arrives from a BGP peer without the Local Pref attribute set. It is overridden by any value set via a route policy.</td>
</tr>
<tr>
<td>Refs</td>
<td>The number of routes using a specified set of path attributes.</td>
</tr>
<tr>
<td>ASes</td>
<td>The number of autonomous system numbers in the AS path attribute.</td>
</tr>
<tr>
<td>Segments</td>
<td>The number of segments in the AS path attribute.</td>
</tr>
<tr>
<td>Flags</td>
<td>EBGP-learned — Path attributes learned by an EBGP peering.</td>
</tr>
<tr>
<td></td>
<td>IBGP-Learned — Path attributes learned by an IBGP peering.</td>
</tr>
<tr>
<td>Aggregator</td>
<td>The route aggregator ID.</td>
</tr>
<tr>
<td>Community</td>
<td>The BGP community attribute list.</td>
</tr>
<tr>
<td>Originator ID</td>
<td>The originator ID path attribute value.</td>
</tr>
<tr>
<td>Cluster List</td>
<td>The route reflector cluster list.</td>
</tr>
</tbody>
</table>

Sample Output

===============================================================================
<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured local AS setting. If not configured, then the value is the same as the AS.</td>
</tr>
<tr>
<td>Path</td>
<td>The AS path attribute.</td>
</tr>
<tr>
<td>Origin</td>
<td>EGP — The NLRI is learned by an EGP protocol.</td>
</tr>
<tr>
<td></td>
<td>IGP — The NLRI is interior to the originating AS.</td>
</tr>
<tr>
<td></td>
<td>INCOMPLETE — NLRI was learned another way.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The advertised BGP nexthop.</td>
</tr>
<tr>
<td>MED</td>
<td>The Multi-Exit Discriminator value.</td>
</tr>
<tr>
<td>Local Preference</td>
<td>The local preference value. This value is used if the BGP route arrives from a BGP peer without the Local Pref attribute set. It is overridden by any value set via a route policy.</td>
</tr>
<tr>
<td>Refs</td>
<td>The number of routes using a specified set of path attributes.</td>
</tr>
<tr>
<td>ASes</td>
<td>The number of autonomous system numbers in the AS path attribute.</td>
</tr>
<tr>
<td>Segments</td>
<td>The number of segments in the AS path attribute.</td>
</tr>
<tr>
<td>Flags</td>
<td>EBGP-learned — Path attributes learned by an EBGP peering.</td>
</tr>
<tr>
<td></td>
<td>IBGP-Learned — Path attributes learned by an IBGP peering.</td>
</tr>
<tr>
<td>Aggregator</td>
<td>The route aggregator ID.</td>
</tr>
<tr>
<td>Community</td>
<td>The BGP community attribute list.</td>
</tr>
<tr>
<td>Originator ID</td>
<td>The originator ID path attribute value.</td>
</tr>
<tr>
<td>Cluster List</td>
<td>The route reflector cluster list.</td>
</tr>
</tbody>
</table>
route-target

Syntax  route-target

Context  show>router>bgp

Description  This command displays a summary of route-target.

Sample Output

*A:Dut-D# show router bgp routes route-target

-----------------------------------------------------------------------------------------------
BGP Router ID: 10.20.1.4  AS: 100  Local AS: 100
-----------------------------------------------------------------------------------------------
Legend -
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes  : i - IGP, e - EGP, ?, incomplete, > - best, b - backup
-----------------------------------------------------------------------------------------------
BGP RT Constrain Routes
-----------------------------------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Flag</th>
<th>Route Target</th>
<th>LocalPref</th>
<th>MED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0:0:0:0</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>u*?</td>
<td>10.10.9.6</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>106 106</td>
<td>1236</td>
<td></td>
</tr>
</tbody>
</table>
-----------------------------------------------------------------------------------------------
routes

Syntax

routes [family] [brief]
routes [family] prefix [detail | longer | hunt [brief]]
routes family prefix [detail | longer | hunt [brief]]
routes [family [type mvpn-type]] community comm-id
routes [family [type mvpn-type]] aspath-regex reg-ex
routes mvpn-ipv4 type mvpn-type (rd rd | originator-ip ip-address | source-ip ip-address | group-ip ip-address | source-as as-number) [hunt| detail]
routes [family [l2vpn-type]] [brief]
routes [family [l2vpn-type]] community comm-id
routes [family [l2vpn-type]] aspath-regex reg-ex
routes l2-vpn l2vpn-type [{rd rd} | {siteid site-id} | {veid veid} [offset vpls-base-offset]}
routes mdt-safi (rd rd) [grp-address mcast-grp-address] [brief]
routes ms-pw [rd rd] [all-type2 all-type2] [brief]
routes flow-ipv4

Context

show>router>bgp

Description

This command displays BGP route information.

When this command is issued without any parameters, then the entire BGP routing table displays.

When this command is issued with an IP prefix/mask or IP address, then the best match for the parameter displays.

Parameters

family — Specify the type of routing information to be distributed by the BGP instance.

Values

ipv4 — Displays only those BGP peers that have the IPv4 family enable and not those capable of exchanging IP-VPN routes.

vpn-ipv4 — Displays the BGP peers that are IP-VPN capable.

mcast-ipv4 — Displays the BGP peers that are mcast-ipv4 capable.

received — Specifies to show the BGP routes received from the neighbor.

prefix — Specifies the type of routing information to display.

Values

Syntax: "rd"|"<rd>:"|<ip-prefix[/ip-prefix-length]>
    comm-val [0..65535]
    2byte-asnumber [0..65535]
    ext-comm-val [0..4294967295]
    4byte-asnumber asn1.asn2 (two 2-byte pieces)
    asn1 - [1..65535]
    asn2 - [0..65535]
    ip-address a.b.c.d
Show Commands

ipv4-prefix a.b.c.d
ipv4-prefix-le [0..32]

**filter** — Specifies route criteria.

**Values**
- **hunt** Displays entries for the specified route in the RIB-In, RIB-Out, and RTM.
- **longer** Displays the specified route and subsets of the route.
- **detail** Display the longer, more detailed version of the output.

**aspath-regexp “reg-exp”** — Displays all routes with an AS path matching the specified regular expression `reg-exp`.

**community comm.-id** — Displays all routes with the specified BGP community.

**Values**
- `[as-number1:comm-val1 | ext-comm | well-known-comm]`
- `ext-comm type: {ip-address:comm-val1 | as-number1:comm-val2 | as-number2:comm-val1}`
- `as-number1 0 — 65535`
- `comm-val1 0 — 65535`
- `type target, origin`
- `ip-address a.b.c.d`
- `comm-val2 0 — 4294967295`
- `as-number2 0 — 4294967295`
- `well-known-comm no-export, no-export-subconfed, no-advertise`

**brief** — Provides a summarized display of the set of peers to which a BGP route is advertised.

**rd** — Specifies the route distinguisher.

**Values**
- `ip-addr:comm-val`
- `2byte-asnumber:ext-comm-val`
- `4byte-asnumber:comm-val`}

**veid** — Specifies a two byte identifier that represents the local bridging instance in a VPLS and is advertised through the BGP NLRI. This value must be lower than or equal to the max-ve-id.

**Values**
- `0 — 4294967295`

**vpls-base-offset** — Specifies a two byte identifier advertised through the NLRI that is used to indicate which VE-ID should use the advertised NLRI at the receiving PE according to the following rule: if the offset <= local VE-ID <= offset+VBS-1 (VBS = virtual block size = 8 in our implementation) then the NLRI is processed. Otherwise it is ignored. The NLRI with this offset is generated as soon as the first VE-ID value between (offset, offset + VBS-1) is advertised in the network.

**Values**
- `0 — 4294967295`

**site-id** — Specifies a two byte identifier usually employed for the BGP multi-homing solution. It identifies the BGP multi-homing site associated with one or a set of objects (SAP(s), pseudowire(s) or combination). The site-id must be identical between the two PEs carrying the connection to the access device multi-homed to the PEs.

**Values**
- `0 — 4294967295`

**l2vpn-type** — Specifies a 12-byte Virtual Switch Instance identifier (VSI-ID) type.

**Values**
- `bgp-ad, bgp-vpls, multi-homing`

**ms-pw** `[rd rd] [aii-type2 aii-type2] [brief]** — Displays routes for ms-pw family.
### BGP Route

The following table describes the command output fields for BGP routes.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured local AS setting. If not configured, then the value is the same as the AS.</td>
</tr>
<tr>
<td>Route Dist.</td>
<td>Displays the route distinguisher identifier attached to routes that distinguishes the VPN it belongs.</td>
</tr>
<tr>
<td>VPN Label</td>
<td>Displays the label generated by the PE's label manager.</td>
</tr>
<tr>
<td>Network</td>
<td>The IP prefix and mask length.</td>
</tr>
<tr>
<td>Nexthop</td>
<td>The BGP nexthop.</td>
</tr>
<tr>
<td>From</td>
<td>The advertising BGP neighbor’s IP address.</td>
</tr>
<tr>
<td>Res. Nexthop</td>
<td>The resolved nexthop.</td>
</tr>
<tr>
<td>Local Pref.</td>
<td>The local preference value. This value is used if the BGP route arrives from a BGP peer without the Local Pref attribute set. It is overridden by any value set via a route policy.</td>
</tr>
<tr>
<td>Flag</td>
<td>u — used</td>
</tr>
<tr>
<td></td>
<td>s — suppressed</td>
</tr>
<tr>
<td></td>
<td>h — history</td>
</tr>
<tr>
<td></td>
<td>d — decayed</td>
</tr>
<tr>
<td></td>
<td>* — valid</td>
</tr>
<tr>
<td></td>
<td>i — igrp</td>
</tr>
<tr>
<td></td>
<td>e — egp</td>
</tr>
<tr>
<td></td>
<td>? — incomplete</td>
</tr>
<tr>
<td></td>
<td>&gt; — best</td>
</tr>
<tr>
<td>Aggregator AS</td>
<td>The aggregator AS value.</td>
</tr>
<tr>
<td></td>
<td>none — Aggregator AS attributes are not present.</td>
</tr>
<tr>
<td>Aggregator</td>
<td>The aggregator attribute value.</td>
</tr>
<tr>
<td></td>
<td>none — Aggregator attributes are not present.</td>
</tr>
</tbody>
</table>
### Sample Output

*A:Dut-C# show router bgp routes l2-vpn detail

<table>
<thead>
<tr>
<th>Label</th>
<th>Description (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atomic Aggr.</td>
<td>Atomic — The atomic aggregator flag is set.</td>
</tr>
<tr>
<td></td>
<td>Not Atomic — The atomic aggregator flag is not set.</td>
</tr>
<tr>
<td>MED</td>
<td>The MED metric value.</td>
</tr>
<tr>
<td></td>
<td>none — MED metrics are present.</td>
</tr>
<tr>
<td>Community</td>
<td>The BGP community attribute list.</td>
</tr>
<tr>
<td>Cluster</td>
<td>The route reflector cluster list.</td>
</tr>
<tr>
<td>Originator Id</td>
<td>The originator ID path attribute value.</td>
</tr>
<tr>
<td></td>
<td>none — The originator ID attribute is not present.</td>
</tr>
<tr>
<td>Peer Router Id</td>
<td>The router ID of the advertising router.</td>
</tr>
<tr>
<td>AS-Path</td>
<td>The BGP AS path attribute.</td>
</tr>
<tr>
<td>VPRN Imported</td>
<td>Displays the VPRNs where a particular BGP-VPN received route has been imported and installed.</td>
</tr>
</tbody>
</table>

Legend -

Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid

Origin codes : i - IGP, e - EGP, ? - incomplete, > - best, b - backup

<table>
<thead>
<tr>
<th>BGP L2VPN Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Type</td>
</tr>
<tr>
<td>Route Dist.</td>
</tr>
<tr>
<td>Prefix</td>
</tr>
</tbody>
</table>
Nexthop : 10.20.1.1
From : 10.20.1.1
Res. Nexthop : n/a
Local Pref. : 100
Aggregator AS : None
Atomic Aggr. : Not Atomic
AIGP Metric : Not Atomic
Cluster : No Cluster Members
Originator Id : None
Flags : Used Valid Best IGP
Route Source : Internal
AS-Path : No As-Path
---
PMSI Tunnel Attribute :
Tunnel-type : RSVP-TE P2MP LSP Flags : Leaf not required
MPLS Label : 0
P2MP-ID : 1001 Tunnel-ID : 61440
Extended-Tunne* : 10.20.1.1

*A:Dut-C# show router bgp routes hunt 1.1.1.1/32

Legend -
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid Origin codes :
i - IGP, e - EGP, ? - incomplete, > - best

BGP IPv4 Routes

RIB In Entries

Network : 1.1.1.1/32
Nexthop : 10.20.1.1
From : 10.20.1.1
Res. Nexthop : 10.20.1.1 (RSVP LSP: 1)
Local Pref. : 100  Interface Name : ip-10.10.2.3
Aggregator AS : None  Aggregator : None
Atomic Aggr. : Not Atomic  MED : None
Community : No Community Members
Cluster : No Cluster Members
Originator Id : None  Peer Router Id : 10.20.1.1
Flags : Used Valid Best Incomplete
AS-Path : No As-Path

RIB Out Entries

Routes : 1

A:ALA-12>config>router:bgp# show router bgp routes family ipv4

BGP Router ID : 10.10.10.103  AS : 200  Local AS : 200

Legend - Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes : i - IGP, e - EGP, ? - incomplete, > - best

BGP Routes

Flag  Network                             Nexthop         LocalPref  MED
VPN Label                           As-Path
-------------------------------------------------------------------------------
No Matching Entries Found
-------------------------------------------------------------------------------

A:ALA-12>config>router:bgp#

A:ALA-12>config>router:bgp# show router bgp routes 13.1.0.0/24 de

BGP Router ID : 10.128.0.161  AS : 65535  Local AS : 65535

Legend - Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes : i - IGP, e - EGP, ? - incomplete, > - best

BGP Routes

Original Attributes
Network : 13.1.0.0/24  Nexthop : 10.20.1.20
Route Dist. : 10070:100  VPN Label : 152784
From : 10.20.1.20  Res. Nexthop : 10.130.0.2
Local Pref. : 100
Aggregator AS: none  Aggregator : none
Atomic Aggr. : Not Atomic  MED : none
Community : target:10070:1
Cluster : No Cluster Members
Originator Id: None  Peer Router Id : 10.20.1.20
Flags : Used Valid Best IGP
AS-Path : 10070 (14730)

Modified Attributes
Network : 13.1.0.0/24    Nexthop : 10.20.1.20
Route Dist. : 10001:100    VPN Label : 152560
From : 10.20.1.20    Res. Nexthop : 10.130.0.2
Local Pref. : 100
Aggregator AS: none    Aggregator : none
Atomic Aggr. : Not Atomic    MED : none
Community : target:10001:1
Cluster : No Cluster Members
Originator Id: None    Peer Router Id : 10.20.1.20
Flags : Used Valid Best IGP
AS-Path : No As-Path
-------------------------------------------------------------------------------

A:ALA-12>config>router:bgp#

A:SR-12# show router bgp routes 100.0.0.0/30 hunt
===============================================================================
BGP Router ID : 10.20.1.1   AS : 100Local AS : 100
===============================================================================
Legend -
Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes  : i - IGP, e - EGP, ? - incomplete, > - best
===============================================================================
BGP Routes
===============================================================================
RIB In Entries
-------------------------------------------------------------------------------
Network : 100.0.0.0/30    Nexthop : 10.20.1.2
Route Dist. : 10.20.1.2:1    VPN Label : 131070
From : 10.20.1.2
Res. Nexthop : 10.10.1.2
Local Pref. : 100    Interface Name: to-sr7
Aggregator AS : none    Aggregator : none
Atomic Aggr. : Not Atomic    MED : none
Community : target:10.20.1.2:1
Cluster : No Cluster Members
Originator Id : None    Peer Router Id : 10.20.1.2
Flags : Used Valid Best IGP
AS-Path : No As-Path
VPRN Imported : 1 2 10 12
-------------------------------------------------------------------------------
RIB Out Entries
-------------------------------------------------------------------------------
Routes : 1
===============================================================================
A:SR-12#

*A:praragon-sim1# /show router bgp routes mvpn-ipv4
===============================================================================
BGP Router ID:10.20.1.3        AS:200         Local AS:200
===============================================================================
Legend -
Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes  : i - IGP, e - EGP, ? - incomplete, > - best
===============================================================================

### BGP MVPN-IPv4 Routes

<table>
<thead>
<tr>
<th>Flag</th>
<th>RouteType</th>
<th>OriginatorIP</th>
<th>LocalPref</th>
<th>MED</th>
<th>RD</th>
<th>SourceAS</th>
<th>Nexthop</th>
<th>As-Path</th>
<th>SourceIP</th>
<th>GroupIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>u*&gt;i</td>
<td>Intra-Ad</td>
<td>10.20.1.4</td>
<td>100</td>
<td>0</td>
<td>1:1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1:1</td>
<td>10.20.1.4</td>
<td>-</td>
<td>No As-Path</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>u*&gt;i</td>
<td>Source-Ad</td>
<td>-</td>
<td>100</td>
<td>0</td>
<td>1:1</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>130.100.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1:1</td>
<td>10.20.1.4</td>
<td>-</td>
<td>No As-Path</td>
<td>227.0.0.0</td>
<td></td>
</tr>
<tr>
<td>u*&gt;i</td>
<td>Source-Join</td>
<td>-</td>
<td>100</td>
<td>0</td>
<td>1:1</td>
<td>200</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>150.100.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1:1</td>
<td>10.20.1.4</td>
<td>-</td>
<td>No As-Path</td>
<td>226.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>

Routes : 3

---

*A:praragon-sim1#* 

*A:praragon-sim1# show router bgp routes mvpn-ipv4 brief*

---

BGP Router ID: 10.20.1.3 AS: 200 Local AS: 200

Legend -
Status codes : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes : i - IGP, e - EGP, ? - incomplete, > - best

BGP MVPN-IPv4 Routes

<table>
<thead>
<tr>
<th>Flag</th>
<th>RouteType</th>
<th>OriginatorIP</th>
<th>SourceIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>u*&gt;i</td>
<td>Intra-Ad</td>
<td>10.20.1.4</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1:1</td>
</tr>
<tr>
<td>u*&gt;i</td>
<td>Source-Ad</td>
<td>-</td>
<td>130.100.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1:1</td>
</tr>
<tr>
<td>u*&gt;i</td>
<td>Source-Join</td>
<td>-</td>
<td>150.100.1.2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1:1</td>
</tr>
</tbody>
</table>

Routes : 3

---

*A:praragon-sim1#* 

*A:praragon-sim1# show router bgp routes mvpn-ipv4 type source-join source-as 200 source-ip 150.100.1.2 group-ip 226.0.0.0 detail*

---
BGP MVPN-IPv4 Routes

<table>
<thead>
<tr>
<th>Route Type</th>
<th>Source-Join</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Dist.</td>
<td>1:1</td>
</tr>
<tr>
<td>Source AS</td>
<td>200</td>
</tr>
<tr>
<td>Source IP</td>
<td>150.100.1.2</td>
</tr>
<tr>
<td>Group IP</td>
<td>226.0.0.0</td>
</tr>
<tr>
<td>Nexthop</td>
<td>10.20.1.4</td>
</tr>
<tr>
<td>From</td>
<td>10.20.1.4</td>
</tr>
<tr>
<td>Res. Nexthop</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Local Pref.</td>
<td>100</td>
</tr>
<tr>
<td>Aggregator AS</td>
<td>None</td>
</tr>
<tr>
<td>Aggregator</td>
<td>None</td>
</tr>
<tr>
<td>Atomic Aggr.</td>
<td>Not Atomic</td>
</tr>
<tr>
<td>Community</td>
<td>target:10.20.1.3:2</td>
</tr>
<tr>
<td>Cluster</td>
<td>No Cluster Members</td>
</tr>
<tr>
<td>Originator Id</td>
<td>None</td>
</tr>
<tr>
<td>Peer Router Id</td>
<td>10.20.1.4</td>
</tr>
<tr>
<td>Flags</td>
<td>Used Valid Best IGP</td>
</tr>
<tr>
<td>AS-Path</td>
<td>No As-Path</td>
</tr>
<tr>
<td>Interface Name</td>
<td>NotAvailable</td>
</tr>
</tbody>
</table>

Routes : 1

*A:praragon-sim1#*

*A:Dut-C# show router bgp routes ms-pw*

---

BGP Router ID: 10.20.1.3        AS: 100         Local AS: 100

Legend -
Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
Origin codes  : i - IGP, e - EGP, ? - incomplete, > - best, b - backup

---

BGP MSPW Routes

<table>
<thead>
<tr>
<th>Flag</th>
<th>Network</th>
<th>RD</th>
<th>AII-Type2/Preflen</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>3:10.20.1.3</td>
<td>100:3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.20.1.5</td>
<td>3:10.20.1.3:0/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>?</td>
<td>3:10.20.1.3</td>
<td>100:4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.20.1.5</td>
<td>3:10.20.1.3:0/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>u*&gt;?</td>
<td>6:10.20.1.6</td>
<td>100:6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.20.1.5</td>
<td>6:10.20.1.6:0/64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>200 300 400</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Routes : 3
### Show Commands

#### summary

**Syntax**

```
summary [all]
summary [family family] [neighbor ip-address]
```

**Context**

```
show>router>bgp
```

**Description**

This command displays a summary of BGP neighbor information.

If confederations are not configured, that portion of the output will not display.

The “State” field displays the global BGP operational state. The valid values are:

- **Up** — BGP global process is configured and running.
- **Down** — BGP global process is administratively shutdown and not running.
- **Disabled** — BGP global process is operationally disabled. The process must be restarted by the operator.

For example, if a BGP peer is operationally disabled, then the state in the summary table shows the state ‘Disabled’

**Parameters**

- **family** — Specify the type of routing information to be distributed by the BGP instance.
  - **Values**
    - ipv4 — Displays only those BGP peers that have the IPv4 family enabled.
    - vpn-ipv4 — Displays the BGP peers that are IP-VPN capable.
    - mcast-ipv4 — Displays the BGP peers that are mcast-ipv4 capable.

- **neighbor ip-address** — Clears damping information for entries received from the BGP neighbor.
  - **Values**
    - ipv4-address: a.b.c.d

**Output**

**BGP Summary Output** — The following table describes the command output fields for a BGP summary.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP Router ID</td>
<td>The local BGP router ID.</td>
</tr>
<tr>
<td>AS</td>
<td>The configured autonomous system number.</td>
</tr>
<tr>
<td>Local AS</td>
<td>The configured local AS setting. If not configured, then the value is the same as the AS.</td>
</tr>
<tr>
<td>BGP Admin State</td>
<td>Down — BGP is administratively disabled.</td>
</tr>
<tr>
<td></td>
<td>Up — BGP is administratively enabled.</td>
</tr>
<tr>
<td>BGP Oper State</td>
<td>Down — BGP is operationally disabled.</td>
</tr>
<tr>
<td></td>
<td>Up — BGP is operationally enabled.</td>
</tr>
<tr>
<td>Bfd</td>
<td>Yes — BFD is enabled.</td>
</tr>
<tr>
<td></td>
<td>No — BFD is disabled.</td>
</tr>
<tr>
<td>Confederation AS</td>
<td>The configured confederation AS.</td>
</tr>
<tr>
<td>Member Confedera-</td>
<td>The configured members of the BGP confederation.</td>
</tr>
<tr>
<td>tions</td>
<td></td>
</tr>
<tr>
<td>Label</td>
<td>Description (Continued)</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of Peer Groups</td>
<td>The total number of configured BGP peer groups.</td>
</tr>
<tr>
<td>Number of Peers</td>
<td>The total number of configured BGP peers.</td>
</tr>
<tr>
<td>Total BGP Active Routes</td>
<td>The total number of BGP routes used in the forwarding table.</td>
</tr>
<tr>
<td>Total BGP Routes</td>
<td>The total number of BGP routes learned from BGP peers.</td>
</tr>
<tr>
<td>Total BGP Paths</td>
<td>The total number of unique sets of BGP path attributes learned from BGP peers.</td>
</tr>
<tr>
<td>Total Path Memory</td>
<td>Total amount of memory used to store the path attributes.</td>
</tr>
<tr>
<td>Total Suppressed Routes</td>
<td>Total number of suppressed routes due to route damping.</td>
</tr>
<tr>
<td>Total History Routes</td>
<td>Total number of routes with history due to route damping.</td>
</tr>
<tr>
<td>Total Decayed Routes</td>
<td>Total number of decayed routes due to route damping.</td>
</tr>
<tr>
<td>Total VPN Peer Groups</td>
<td>The total number of configured VPN peer groups.</td>
</tr>
<tr>
<td>Total VPN Peers</td>
<td>The total number of configured VPN peers.</td>
</tr>
<tr>
<td>Total VPN Local Rts</td>
<td>The total number of configured local VPN routes.</td>
</tr>
<tr>
<td>Total VPN Remote Rts</td>
<td>The total number of configured remote VPN routes.</td>
</tr>
<tr>
<td>Total VPN Remote Active Rts.</td>
<td>The total number of active remote VPN routes used in the forwarding table.</td>
</tr>
<tr>
<td>Total VPN Supp.Rts.</td>
<td>Total number of suppressed VPN routes due to route damping.</td>
</tr>
<tr>
<td>Total VPN Hist. Rts.</td>
<td>Total number of VPN routes with history due to route damping.</td>
</tr>
<tr>
<td>Total VPN Decay Rts.</td>
<td>Total number of decayed routes due to route damping.</td>
</tr>
<tr>
<td>Neighbor</td>
<td>BGP neighbor address.</td>
</tr>
<tr>
<td>AS (Neighbor)</td>
<td>BGP neighbor autonomous system number.</td>
</tr>
<tr>
<td>PktRcvd</td>
<td>Total number of packets received from the BGP neighbor.</td>
</tr>
<tr>
<td>PktSent</td>
<td>Total number of packets sent to the BGP neighbor.</td>
</tr>
<tr>
<td>InQ</td>
<td>The number of BGP messages to be processed.</td>
</tr>
</tbody>
</table>
Show Commands

**Sample Output**

A: SetupCLI>show>router# bgp summary

```
BGP Router ID : 21.3.4.5          AS : 35012   Local AS : 100
Confederation AS        : 40000  Member Confederations   : 35012 65205 65206 65207 65208
Rapid Withdrawal        : Disabled  Bfd Enabled             : Yes
Number of Peer Groups   : 1           Number of Peers             : 1
Total BGP Paths         : 3           Total Path Memory           : 396
Total BGP Active Rts.   : 0           Total BGP Rts.              : 0
Total Supressed Rts.    : 0           Total Hist. Rts.            : 0
Total Decay Rts.        : 0
Total VPN Peer Groups   : 1           Total VPN Peers             : 1
Total VPN Local Rts.    : 0
Total VPN Remote Rts.   : 0           Total VPN Remote Active Rts.: 0
Total VPN Supp. Rts.    : 0           Total VPN Hist. Rts.         : 0
Total VPN Decay Rts.    : 0
```

BGP Summary

```
Neighbor  AS  PktRcvd InQ  Up/Down  State|Recv/Actv/Sent (IPv4)  Rcv/Act/Sent (VpnIPv4)  Rcv/Act/Sent (MacastIPv4)
PktSent  OutQ
3.3.3.3    20  0  0  01h55m56s Active  0  0
```

A: SetupCLI>show>router#
Syntax

mvpn

Context

show>router

Description

This command displays Multicast VPN related information.

Sample Output

*A:praragon-sim1# show router 100 mvpn
===============================================================================
MVPN 100 configuration data
===============================================================================
i-pmsi             : 224.100.201.101 ssm  admin status       : Up
hello-interval     : 30 seconds           hello-multiplier   : 35 * 0.1
three-way-hello    : Disabled             tracking support   : Disabled
s-pmsi range       : 0.0.0.0/0            data-delay-interval: 3 seconds
join-tlv-packing   : N/A
signaling          : Bgp
vrf-import         : N/A
vrf-export         : N/A
vrf-target         : N/A
===============================================================================
*A:praragon-sim1#
Clear Commands

**damping**

**Syntax**
```
damping [[ip-prefix/ip-prefix-length] [neighbor ip-address]] | [group name]
```

**Context**
clear>router>bgp

**Description**
This command clears or resets the route damping information for received routes.

**Parameters**
- `ip-prefix/ip-prefix-length` — Clears damping information for entries that match the IP prefix and prefix length.
  
  **Values**
  - `ipv4-prefix`: a.b.c.d (host bits must be 0)
  - `ipv4-prefix-length`: 0 — 328

- `neighbor ip-address` — Clears damping information for entries received from the BGP neighbor.
  
  **Values**
  - `ipv4-address`: a.b.c.d

- `group name` — Clears damping information for entries received from any BGP neighbors in the peer group.
  
  **Values**
  - 32 characters maximum

**flap-statistics**

**Syntax**
```
flap-statistics [[ip-prefix/mask] [neighbor ip-address]] | [group group-name] | [regex reg-exp] | [policy policy-name]
```

**Context**
clear>router>bgp

**Description**
This command clears route flap statistics.

**Parameters**
- `ip-prefix/mask` — Clears route flap statistics for entries that match the specified IP prefix and mask length.
  
  **Values**
  - `ip-prefix`: a.b.c.d (host bits must be 0)
  - `mask`: 0 — 32

- `neighbor ip-address` — Clears route flap statistics for entries received from the specified BGP neighbor.
  
  **Values**
  - `ipv4-address`: a.b.c.d

- `group group-name` — Clears route flap statistics for entries received from any BGP neighbors in the specified peer group.

- `regex reg-exp` — Clears route flap statistics for all entries which have the regular expression and the AS path that matches the regular expression.

- `policy policy-name` — Clears route flap statistics for entries that match the specified route policy.
neighbor

Syntax \texttt{neighbor \{ip-address | as as-number | external | all\} [soft | soft-inbound]}
neighbor(ip-address | as as-number | external | all) statistics
neighbor ip-address end-of-rib

Context clear>router>bgp

Description This command resets the specified BGP peer or peers. This can cause existing BGP connections to be shutdown and restarted.

Parameters \texttt{ip-address} — Resets the BGP neighbor with the specified IP address.

\textbf{Values} \quad ipv4-address: \quad a.b.c.d

\texttt{as as-number} — Resets all BGP neighbors with the specified peer AS.

\textbf{Values} \quad 1 — 65535

\texttt{external} — Resets all EBGP neighbors.

\texttt{all} — Resets all BGP neighbors.

\texttt{soft} — The specified BGP neighbor(s) re-evaluates all routes in the Local-RIB against the configured export policies.

\texttt{soft-inbound} — The specified BGP neighbor(s) re-evaluates all routes in the RIB-In against the configured import policies.

\texttt{statistics} — The BGP neighbor statistics.

\texttt{end-of-rib} — Clears the routing information base (RIB). This command applies when the SR OS node is helping the BGP neighbor through a BGP graceful restart. When the \texttt{clear router bgp neighbor} command is issued without the end-of-rib option and the neighbor is in the process of restarting, stale routes from the neighbor will be retained until the stale-routes-time is reached or else the neighbor exits graceful restart. When the command is issued with the end-of-rib option, stale routes from the neighbor are deleted immediately and graceful restart procedures are aborted.

protocol

Syntax \texttt{protocol}

Context clear>router>bgp

Description Resets the entire BGP protocol.
Debug Commands

events

Syntax  
```bash
events [neighbor ip-address | group name]
```

no events

Context  
debug>router>bgp

Description  
This command logs all events changing the state of a BGP peer.

Parameters
- **neighbor ip-address** — Debugs only events affecting the specified BGP neighbor.
  - Values  
    - ipv4-address: a.b.c.d (host bits must be 0)
  - **group name** — Debugs only events affecting the specified peer group and associated neighbors.

graceful-restart

Syntax  
```bash
graceful-restart [neighbor ip-address | group name]
```

no graceful-restart

Context  
debug>router>bgp

Description  
This command enables debugging for BGP graceful-restart.
The no form of the command disables the debugging.

Parameters
- **neighbor ip-address** — Debugs only events affecting the specified BGP neighbor.
  - Values  
    - ipv4-address: a.b.c.d (host bits must be 0)
  - **group name** — Debugs only events affecting the specified peer group and associated neighbors.

keepalive

Syntax  
```bash
keepalive [neighbor ip-addr | group name]
```

no keepalive

Context  
debug>router>bgp

Description  
This command decodes and logs all sent and received keepalive messages in the debug log.

Parameters
- **neighbor ip-address** — Debugs only events affecting the specified BGP neighbor.
  - Values  
    - ipv4-address: a.b.c.d (host bits must be 0)
  - **group name** — Debugs only events affecting the specified peer group and associated neighbors.
notification

Syntax  

```
notification [neighbor ip-address | group name]
no notification
```

Context  
debug>router>bgp

Description  
This command decodes and logs all sent and received notification messages in the debug log.

Parameters  
neighbor ip-address — Debugs only events affecting the specified BGP neighbor.

Values  
ipv4-address: a.b.c.d (host bits must be 0)

group name — Debugs only events affecting the specified peer group and associated neighbors.

open

Syntax  

```
open [neighbor ip-address | group name]
no open
```

Context  
debug>router>bgp

Description  
This command decodes and logs all sent and received open messages in the debug log.

Parameters  
neighbor ip-address — Debugs only events affecting the specified BGP neighbor.

Values  
ipv4-address: a.b.c.d (host bits must be 0)

group name — Debugs only events affecting the specified peer group and associated neighbors.

outbound-route-filtering

Syntax  

```
[no] outbound-route-filtering
```

Context  
debug>router>bgp

Description  
This command enables debugging for all BGP outbound route filtering (ORF) packets. ORF is used to inform a neighbor of targets (using target-list) that it is willing to receive.

packets

Syntax  

```
packets [neighbor ip-address | group name]
packets
```

Context  
debug>router>bgp

Description  
This command decodes and logs all sent and received BGP packets in the debug log.
Debug Commands

Parameters

neighbor ip-address — Debugs only events affecting the specified BGP neighbor.

Values

- ipv4-address: a.b.c.d (host bits must be 0)

group name — Debugs only events affecting the specified peer group and associated neighbors.

route-refresh

Syntax

route-refresh [neighbor ip-address | group name]

no route-refresh

Context debug>router>bgp

Description

This command enables and disables debugging for BGP route-refresh.

Parameters

neighbor ip-address — Debugs only events affecting the specified BGP neighbor.

Values

- ipv4-address: a.b.c.d (host bits must be 0)

group name — Debugs only events affecting the specified peer group and associated neighbors.

rtm

Syntax

rtm [neighbor ip-address | group name]

no rtm

Context debug>router>bgp

Description

This command logs RTM changes in the debug log.

Parameters

neighbor ip-address — Debugs only events affecting the specified BGP neighbor.

Values

- ipv4-address: a.b.c.d (host bits must be 0)

group name — Debugs only events affecting the specified peer group and associated neighbors.

socket

Syntax

socket [neighbor ip-address | group name]

no socket

Context debug>router>bgp

Description

This command logs all TCP socket events to the debug log.

Parameters

neighbor ip-address — Debugs only events affecting the specified BGP neighbor.

Values

- ipv4-address: a.b.c.d (host bits must be 0)

group name — Debugs only events affecting the specified peer group and associated neighbors.
timers

Syntax: timers [neighbor ip-address | group name]
no timers

Context: debug>router:bgp

Description: This command logs all BGP timer events to the debug log.

Parameters:
- **neighbor ip-address** — Debugs only events affecting the specified BGP neighbor.
  - Values: ipv4-address: a.b.c.d (host bits must be 0)
- **group name** — Debugs only events affecting the specified peer group and associated neighbors.

update

Syntax: update [neighbor ip-address | group name]
no update

Context: debug>router:bgp

Description: This command decodes and logs all sent and received update messages in the debug log.

Parameters:
- **neighbor ip-address** — Debugs only events affecting the specified BGP neighbor.
  - Values: ipv4-address: a.b.c.d (host bits must be 0)
- **group name** — Debugs only events affecting the specified peer group and associated neighbors.
In This Chapter

This chapter provides information about configuring route policies.

Topics in this chapter include:

- Configuring Route Policies on page 704
  - Policy Statements on page 705
    - Default Action Behavior on page 706
  - BGP and OSPF Route Policy Support on page 714
    - BGP Route Policies on page 715
    - Re-advertised Route Policies on page 716
    - Triggered Policies on page 716
  - When to Use Route Policies on page 718
- Route Policy Configuration Process Overview on page 719
- Configuration Notes on page 720
Configuring Route Policies

Alcatel-Lucent’s router supports two databases for routing information. The routing database is composed of the routing information learned by the routing protocols. The forwarding database is composed of the routes actually used to forward traffic through a router. In addition, link state databases are maintained by interior gateway protocols (IGPs) such as IS-IS and OSPF.

Routing protocols calculate the best route to each destination and place these routes in a forwarding table. The routes in the forwarding table are used to forward routing protocol traffic, sending advertisements to neighbors and peers.

A routing policy can be configured that will not place routes associated with a specific origin in the routing table. Those routes will not be used to forward data packets to the intended destinations and the routes are not advertised by the routing protocol to neighbors and peers.

Routing policies control the size and content of the routing tables, the routes that are advertised, and the best route to take to reach a destination. Careful planning is essential to implement route policies that can affect the flow of routing information or packets in and traversing through the router. Before configuring and applying a route policy, develop an overall plan and strategy to accomplish your intended routing actions.

There are no default route policies. Each policy must be created explicitly and applied to a routing protocol or to the forwarding table. Policy parameters are modifiable.
Policy Statements

Route policies contain policy statements containing ordered entries containing match conditions and actions you specify. The entries should be sequenced from the most explicit to least explicit. Packet forwarding and routing can be implemented according to your defined policies. Policy-based routing allows you to dictate where traffic can be routed, through specific paths, or whether to forward or drop the traffic. Route policies can match a given route policy entry and continue searching for other matches within either the same route policy or the next route policy.

The process can stop when the first complete match is found and executes the action defined in the entry, either to accept or reject packets that match the criteria or proceed to the next entry or the next policy. You can specify matching criteria based on source, destination, or particular properties of a route. Route policies can be constructed to support multiple stages to the evaluation and setting various route attributes. You can also provide more matching conditions by specifying criteria such as:

- Autonomous system (AS) path policy options — A combination of AS numbers and regular expression operators.
- Community list — A group sharing a common property.
- Prefix list — A named list of prefixes.
- To and From criteria — A route’s source and destination.
Default Action Behavior

The default action specifies how packets are to be processed when a policy related to the route is not explicitly configured. The following default actions are applied in the event that:

- A route policy does not specify a matching condition, all the routes being compared with the route policy are considered to be matches.
- A packet does not match any policy entries, then the next policy is evaluated. If a match does not occur then the last entry in the last policy is evaluated.
- If no default action is specified, the default behavior of the protocol controls whether the routes match or not.

If a default action is defined for one or more of the configured route policies, then the default action is handled as follows:

- The default action can be set to all available action states including accept, reject, next-entry, and next-policy.
- If the action states accept or reject, then the policy evaluation terminates and the appropriate result is returned.
- If a default action is defined and no matches occurred with the entries in the policy, then the default action is used.
- If a default action is defined and one or more matches occurred with the entries of the policy, then the default action is not used.

Denied IP Prefixes

The following IP address prefixes are not allowed by the routing protocols and the Route Table Manager and are not be populated within the forwarding table:

- 0.0.0.0/8 or longer
- 127.0.0.0/8 or longer
- 224.0.0.0/4 or longer
- 240.0.0.0/4 or longer

Any other prefixes that need to be filtered can be filtered explicitly using route policies.
Controlling Route Flapping

Route damping is a controlled acceptance of unstable routes from BGP peers so that any ripple effect caused by route flapping across BGP AS border routers is minimized. The motive is to delay the use of unstable routes (flapping routes) to forward data and advertisements until the route stabilizes.

Alcatel-Lucent’s implementation of route damping is based on the following parameters:

- Figure of Merit — A route is assigned a Figure of Merit (FoM), which is proportional to the frequency of flaps. FoM should be able to characterize a route’s behavior over a period of time.
- Route flap — A route flap is not limited to the withdrawn route. It also applies to any change in the AS path or the next hop of a reachable route. A change in AS path or next hop indicates that the intermediate AS or the route-advertising peer is not suppressing flapping routes at the source or during the propagation. Even if the route is accepted as a stable route, the data packets destined to the route could experience unstable routing due to the unstable AS path or next hop.
- Suppress threshold — The threshold is a configured value that, when exceeded, the route is suppressed and not advertised to other peers. The state is considered to be down from the perspective of the routing protocol.
- Reuse threshold — When FoM value falls below a configured reuse threshold and the route is still reachable, the route is advertised to other peers. The FoM value decays exponentially after a route is suppressed. This requires the BGP implementation to decay thousands of routes from a misbehaving peer.

The two events that could trigger the route flapping algorithm are:

- Route flapping — If a route flap is detected within a configured maximum route flap history time, the route’s FoM is initialized and the route is marked as a potentially unstable route. Every time a route flaps, the FoM is increased and the route is suppressed if the FoM crosses the suppress threshold.
- Route reuse timer trigger — A suppressed route’s FoM decays exponentially. When it crosses the reuse threshold, the route is eligible for advertisement if it is still reachable.

If the route continues to flap, the FoM, with respect to time scale, looks like a sawtooth waveform with the exponential rise and decay of FoM. To control flapping, the following parameters can be configured:

- half-life — The half life value is the time, expressed in minutes, required for a route to remain stable in order for one half of the FoM value to be reduced. For example, if the half life value is 6 (minutes) and the route remains stable for 6 minutes, then the new FoM
value is 3. After another 6 minutes passes and the route remains stable, the new FoM value is 1.5.

- **max-suppress** — The maximum suppression time, expressed in minutes, is the maximum amount of time that a route can remain suppressed.

- **suppress** — If the FoM value exceeds the configured integer value, the route is suppressed for use or inclusion in advertisements.

- **reuse** — If the suppress value falls below the configured reuse value, then the route can be reused.
Regular Expressions

The ability to perform a filter match on confederations in the AS-PATH is supported. This feature allows customers to configure match criteria for specific confederation sets and sequences within the AS path so that they can be filtered out before cluttering the service provider’s routing information base (RIB).

SR OS uses regular expression strings to specify match criteria for:

- An AS path string; for example, “100 200 300”
- A community string; for example, “100:200” where 100 is the AS number, and 200 is the community-value.
- Any AS path beginning with a confederation SET or SEQ containing 65001 and 65002 only: for example “< 65001 65002 >.*”
- Any AS path containing a confederation SET or SEQ, regardless of the contents: for example, “.* <.*> .*”

A regular expression is expressed in terms of terms and operators. A term for an AS path regular expression is:

1. Regular expressions should always be enclosed in quotes.
2. An elementary term; for example, an AS number “200”
3. A range term composed of two elementary terms separated by the ‘-’ character like “200-300”.
4. The ‘.’ dot wild-card character which matches any elementary term.
5. A regular expression enclosed in parenthesis “( )”.
6. A regular expression enclosed in square brackets used to specify a set of choices of elementary or range terms; for example, [100-300 400] matches any AS number between 100 and 300 or the AS number 400.
A term for a community string regular expression is a string that is evaluated character by character and is composed of:

1. An elementary term which for a community string is any single digit like “4”.
2. A range term composed of two elementary terms separated by the ‘-’ character like “2-3”.
3. A colon ‘:’ to delimit the AS number from the community value.
4. The ‘.’ dot wild-card character which matches any elementary term or ‘:’.
5. A regular expression enclosed in parenthesis “( )”.
6. A regular expression enclosed in square brackets used to specify a set of choices of elementary or range terms; for example, [1-37] matches any single digit between 1 and 3 or the digit 7.

The regular expression OPERATORS are listed in Table 20.

### Table 20: Regular Expression Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Matches the term on alternate sides of the pipe.</td>
</tr>
<tr>
<td>*</td>
<td>Matches multiple occurrences of the term.</td>
</tr>
<tr>
<td>?</td>
<td>Matches 0 or 1 occurrence of the term.</td>
</tr>
<tr>
<td>+</td>
<td>Matches 1 or more occurrence of the term.</td>
</tr>
<tr>
<td>( )</td>
<td>Used to parenthesize so a regular expression is considered as one term.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Used to demarcate a set of elementary or range terms.</td>
</tr>
<tr>
<td>-</td>
<td>Used between the start and end of a range.</td>
</tr>
<tr>
<td>{m, n}</td>
<td>Matches least $m$ and at most $n$ repetitions of the term.</td>
</tr>
<tr>
<td>{m}</td>
<td>Matches exactly $m$ repetitions of the term.</td>
</tr>
<tr>
<td>{m,}</td>
<td>Matches $m$ or more repetitions of the term.</td>
</tr>
<tr>
<td>^</td>
<td>Matches the beginning of the string - only allowed for communities.</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of the string - only allowed for communities.</td>
</tr>
<tr>
<td>\</td>
<td>An escape character to indicate that the following character is a match criteria and not a grouping delimiter.</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>Matches any AS path numbers containing a confederation SET or SEQ.</td>
</tr>
</tbody>
</table>
Examples of AS path and community string regular expressions are listed in Table 21.

**Table 21: AS Path and Community Regular Expression Examples**

<table>
<thead>
<tr>
<th>AS Path to Match Criteria</th>
<th>Regular Expression</th>
<th>Example Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null AS path</td>
<td>nulla</td>
<td>Null AS path</td>
</tr>
<tr>
<td>AS path is 11</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>AS path is 11 22 33</td>
<td>11 22 33</td>
<td>11 22 33</td>
</tr>
<tr>
<td>Zero or more occurrences of AS number 11</td>
<td>11*</td>
<td>Null AS path</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 ... 11</td>
</tr>
<tr>
<td>Path of any length that begins with AS numbers 11, 22, 33</td>
<td>11 22 33 .*</td>
<td>11 22 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 22 33 400 500 600</td>
</tr>
<tr>
<td>Path of any length that ends with AS numbers 44, 55, 66</td>
<td>.* 44 55 66</td>
<td>44 55 66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 44 55 66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 200 44 55 66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 200 300 44 55 66</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 200 300 ... 44 55 66</td>
</tr>
<tr>
<td>One occurrence of the AS numbers 100 and 200, followed by one or more occurrences of the number 33</td>
<td>100 200 33+</td>
<td>100 200 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 200 33 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 200 33 33 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 200 33 33 33 33</td>
</tr>
<tr>
<td>One or more occurrences of AS number 11, followed by one or more occurrences of AS number 22, followed by one or more occurrences of AS number 33</td>
<td>11+ 22+ 33+</td>
<td>11 22 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 22 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 22 22 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 22 22 33 33</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 ... 11 22 ... 22 33 ... 33</td>
</tr>
<tr>
<td>Path whose second AS number must be 11 or 22</td>
<td>(. 11)</td>
<td>100 11</td>
</tr>
<tr>
<td></td>
<td>.* or (. 22) .*</td>
<td>200 22 300 400</td>
</tr>
<tr>
<td></td>
<td>. (11</td>
<td>22) .*</td>
</tr>
<tr>
<td>Path of length one or two whose second AS number might be 11 or 22</td>
<td>. (11</td>
<td>22)?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>200 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>300 22</td>
</tr>
</tbody>
</table>
### Table 21: AS Path and Community Regular Expression Examples (Continued)

<table>
<thead>
<tr>
<th>AS Path to Match Criteria</th>
<th>Regular Expression</th>
<th>Example Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path whose first AS number is 100 and second AS number is either 11 or 22</td>
<td>100 (11</td>
<td>22).*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 22 200 300</td>
</tr>
<tr>
<td>Either AS path 11, 22, or 33</td>
<td>[11 22 33]</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>33</td>
</tr>
<tr>
<td>Range of AS numbers to match a single AS number</td>
<td>10-14</td>
<td>10 or 11 or 12 or 13 or 14</td>
</tr>
<tr>
<td></td>
<td>[10-12]*</td>
<td>Null AS path</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 or 11 or 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 10 or 10 11 or 10 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 10 or 11 11 or 11 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12 10 or 12 11 or 12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>Zero or one occurrence of AS number 11</td>
<td>11? or 11{0,1}</td>
<td>Null AS path</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11</td>
</tr>
<tr>
<td>One through four occurrences of AS number 11</td>
<td>11{1,4}</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 11 11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 11 11 11</td>
</tr>
<tr>
<td>One through four occurrences of AS number 11 followed by one occurrence of AS number 22</td>
<td>11{1,4} 22</td>
<td>11 22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 11 22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 11 11 11 22</td>
</tr>
<tr>
<td>Path of any length, except nonexistent, whose second AS number can be anything, including nonexistent</td>
<td>.* or .{0,}</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100 200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11 22 33 44 55</td>
</tr>
<tr>
<td>AS number is 100. Community value is 200.</td>
<td>^100:200$</td>
<td>100:200</td>
</tr>
<tr>
<td>AS number is 11 or 22. Community value is any number.</td>
<td>^((11)</td>
<td>(22)):(.* $</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22:100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11:200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>AS number is 11. Community value is any number that starts with 1.</td>
<td>^11:(1.*)$</td>
<td>11:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11:100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11:1100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
## Table 21: AS Path and Community Regular Expression Examples (Continued)

<table>
<thead>
<tr>
<th>AS Path to Match Criteria</th>
<th>Regular Expression</th>
<th>Example Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS number is any number. Community value is any number that ends with 1, 2, or 3.</td>
<td>^(.<em>) : (.</em>) [1-3]$</td>
<td>11:1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100:2002</td>
</tr>
<tr>
<td></td>
<td></td>
<td>333:55553</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>AS number is 11 or 22. Community value is any number that starts with 3 and ends with 4, 5 or 9.</td>
<td>^((11)</td>
<td>(22)) : (3 .* [459]$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22:3335</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11:3777779</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
<tr>
<td>AS number is 11 or 22. Community value ends in 33 or 44.</td>
<td>[^((11</td>
<td>22)) : (.*) ((33)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22:99944</td>
</tr>
<tr>
<td></td>
<td></td>
<td>22:555533</td>
</tr>
<tr>
<td></td>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>

a. The null keyword matches an empty AS path.
BGP and OSPF Route Policy Support

OSPF and BGP requires route policy support. Figure 27 and Figure 29 display where route policies are evaluated in the protocol. Figure 27 depicts BGP which applies a route policy as an internal part of the BGP route selection process. Figure 29 depicts OSPF which applies routing policies at the edge of the protocol, to control only the routes that are announced to or accepted from the Route Table Manager (RTM).

![Figure 27: BGP Route Policy Diagram](image-url)
BGP Route Policies

Alcatel-Lucent’s implementation of BGP uses route policies extensively. The implied or default route policies can be overridden by customized route policies. The default BGP properties, with no route policies configured, behave as follows:

- Accept all BGP routes into the RTM for consideration.
- Announce all used BGP learned routes to other BGP peers
- Announce none of the IGP, static or local routes to BGP peers.

Figure 28: BGP Route Policy Diagram
Re-advertised Route Policies

Occasionally, BGP routes may be readvertised from BGP into OSPF, IS-IS, and RIP. OSPF export policies (policies control which routes are exported to OSPF) are not handled by the main OSPF task but are handled by a separate task or an RTM task that filters the routes before they are presented to the main OSPF task.

Triggered Policies

With triggered policy enabled, deletion and re-addition of a peer after making changes to export policy causes the new updates sent out to all peers

Triggered policy is not honored if a new peer added to BGP. Update with the old policy is sent to the newly added peer. New policy does not get applied to the new peer until the peer is flapped.

With triggered policy enabled, if a new bgp/static route comes in, new addition or modification of an export policy causes the updates to sent out dynamically to all peers with the new/modified export policy

When multiple peers, say P1, P2 and P3 share the same export policy, any modifications to export policy followed by clear soft on one of the peer P1, will send out routes to P1 only according to newly modified policy.

Though routes with newly modified policy are not sent to other peers (P2, and P3) as no clear soft issues on these peers, RIB-OUT will show that new routes with modified policy are sent to all the peers. RIB-IN on peers P2 and P3 are shown correctly.
Set MED to IGP Cost using Route Policies

This feature sets MED to the IGP cost of a route exported into BGP as an action in route policies. The `med-out` command in the bgp, group, and neighbor configuration context supports this option, but this method lacks per-prefix granularity. The enhanced `metric` command supported as a route policy action supports setting MED to a fixed number, or adding, or subtracting a fixed number from the received MED, and sets IGP cost option. The enhanced `metric {set {igp | number 1} | {add | subtract} number2 }` command is under `config>router>policy-options>policy-statement>entry>action`.

The `metric set igp` command, when used in a BGP export policy, have the same effect as the current `med-out igp` command, except that it applies only to the routes matched by the policy entry.

The effect of the metric set igp command depends on the route type and policy type as summarized in Table 22.

<table>
<thead>
<tr>
<th>BGP Policy Type</th>
<th>Matched Route Type</th>
<th>Set Metric IGP Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export</td>
<td>Non-BGP route (static, OSPF, ISIS, etc.)</td>
<td>Add MED attribute. Set value to M.</td>
</tr>
<tr>
<td>Export</td>
<td>BGP route w/o MED</td>
<td>Add MED attribute. Set value to D.</td>
</tr>
<tr>
<td>Export</td>
<td>BGP route with MED (value A)</td>
<td>Overwrite MED attribute with value D.</td>
</tr>
</tbody>
</table>
When to Use Route Policies

The following are examples of circumstances of when to configure and apply unique route policies.

- When you want to control the protocol to allow all routes to be imported into the routing table. This enables the routing table to learn about particular routes to enable packet forwarding and redistributing packets into other routing protocols.
- When you want to control the exporting of a protocol’s learned active routes.
- When you want a routing protocol to announce active routes learned from another routing protocol, which is sometimes called route redistribution.
- When you want unique behaviors to control route characteristics. For example, change the route preference.
- When you want unique behaviors to control route characteristics. For example, change the route preference, AS path, or community values to manipulate the control the route selection.
- When you want to control BGP route flapping (damping).
Route Policy Configuration Process Overview

Figure 30 displays the process to provision basic route policy parameters.

Figure 30: Route Policy Configuration and Implementation Flow
Configuration Notes

This section describes route policy configuration caveats.

General

• When configuring policy statements, the policy statement name must be unique.
Configuring Route Policies with CLI

This section provides information to configure route policies using the command line interface.

Topics in this section include:

- Route Policy Configuration Overview on page 722
  - When to Create Routing Policies on page 722
  - Policy Evaluation on page 724
  - Damping on page 727

- Configuring Route Policy Components on page 730
  - Creating a Route Policy on page 732
  - Beginning the Policy Statement on page 731
  - Configuring an Entry on page 734
  - Configuring a Community List on page 735
  - Configuring Damping on page 736
  - Configuring a Prefix List on page 737
  - Configuring PIM Join/Register Policies on page 738

- Route Policy Configuration Management Tasks on page 741
Route Policy Configuration Overview

Route policies allow you to configure routing according to specifically defined policies. You can create policies and entries to allow or deny paths based on various parameters such as destination address, protocol, packet size, and community list.

Policies can be as simple or complex as required. A simple policy can block routes for a specific location or IP address. More complex policies can be configured using numerous policy statement entries containing matching conditions to specify whether to accept or reject the route, control how a series of policies are evaluated, and manipulate the characteristics associated with a route.

When to Create Routing Policies

Route policies are created in the config>router context. There are no default route policies. Each route policy must be explicitly created and applied. Applying route policies can introduce more efficiency as well as more complexity to routers’ capabilities.

A route policy impacts the flow of routing information or packets within and through the router. A routing policy can be specified to prevent a particular customer’s routes to be placed in the route table which causes those routes to not forward traffic to various destinations and the routes are not advertised by the routing protocol to neighbors.

Route policies can be created to control:

- A protocol to export all the active routes learned by that protocol.
- Route characteristics to control which route is selected to act as the active route to reach a destination and advertise the route to neighbors.
- Protocol to import all routes into the routing table. A routing table must learn about particular routes to be able to forward packets and redistribute to other routing protocols.
- Damping.

Before a route policy is applied, analyze the policy’s purpose and be aware of the results (and consequences) when packets match the specified criteria and the associated actions and default actions, if specified, are executed. Membership reports can be filtered based on a specific source address.
Default Route Policy Actions

Each routing protocol has default behaviors for the import and export of routing information. Table 23 shows the default behavior for each routing protocol.

Table 23: Default Route Policy Actions

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Import</th>
<th>Export</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF</td>
<td>Not applicable. All OSPF routes are accepted from OSPF neighbors and cannot be controlled via route policies.</td>
<td>• Internal routes: All OSPF routes are automatically advertised to all neighbors. • External routes: By default all non-OSPF learned routes are not advertised to OSPF neighbors</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Not applicable. All IS-IS routes are accepted from IS-IS neighbors and can not be controlled via route policies</td>
<td>• Internal routes: All IS-IS routes are automatically advertised to all neighbors. • External routes: By default all non-IS-IS learned routes are not advertised to IS-IS peers.</td>
</tr>
<tr>
<td>RIP</td>
<td>By default, all RIP-learned routes are accepted.</td>
<td>• External routes: By default all non-RIP learned routes are not advertised to RIP peers.</td>
</tr>
<tr>
<td>BGP</td>
<td>By default, all routes from BGP peers are accepted and passed to the BGP route selection process.</td>
<td>• Internal routes: By default all active BGP routes are advertised to BGP peers • External routes: By default all non-BGP learned routes are not advertised to BGP peers.</td>
</tr>
</tbody>
</table>
Policy Evaluation

Routing policy statements can consist of as few as one or several entries. The entries specify the matching criteria. A route is compared to the first entry in the policy statement. If it matches, the specified entry action is taken, either accepted or rejected. If the action is to accept or reject the route, that action is taken and the evaluation of the route ends.

If the route does not match the first entry, the route is compared to the next entry (if more than one is configured) in the policy statement. If there is a match with the second entry, the specified action is taken. If the action is to accept or reject the route, that action is taken and the evaluation of the route ends, and so on.

Each route policy statement can have a default-action clause defined. If a default-action is defined for one or more of the configured route policies, then the default actions should be handled in the following ways:

• The process stops when the first complete match is found and executes the action defined in the entry.
• If the packet does not match any of the entries, the system executes the default action specified in the policy statement.

Figure 31 depicts an example of the route policy process.

Route policies can also match a given route policy entry and continue to search for other entries within either the same route policy or the next route policy by specifying the next-entry or next-policy option in the entry’s action command. Policies can be constructed to support multiple states to the evaluation and setting of various route attributes.

Figure 32 depicts the next-policy and next-entry route processes.
Figure 31: Route Policy Process Example
Figure 32: Next Policy Logic Example
Damping

Damping initiates controls when routes flap. Route flapping can occur when an advertised route between nodes alternates (flaps) back and forth between two paths due to network problems which cause intermittent route failures. It is necessary to reduce the amount of routing state change updates propagated in order to limit processing requirements. Thus, when a route flaps beyond a configured value (the suppress value), then that route is removed from the routing tables and routing protocols until the value falls below the reuse value.

A route can be suppressed according to the Figure of Merit (FoM) value. The FoM is a value that is added to a route each time it flaps. A new route begins with an FoM value of 0.

Damping is optional. If damping is configured, the following parameter values must be explicitly specified as there are no default values:

- suppress
- half-life
- reuse
- max-suppress

When a route's FoM value exceeds the suppress value, then the route is removed from the routing table. The route is considered to be stable when the FoM drops below the reuse value by means of the specified half life parameter. The route is returned to the routing tables. When routes have higher FoM and half life values, they are suppressed for longer periods of time. Figure 33 depicts an example of a flapping route, the suppress threshold, the half life decay (time), and reuse threshold. The peaks represent route flaps, the slopes represent half life decay.

![Figure 33: Damping Example](image-url)
Basic Configurations

This section provides information to configure route policies and configuration examples of common tasks. The minimal route policy parameters that need to be configured are:

- Policy statement with the following parameters specified:
  - At least one entry
  - Entry action

Following is a sample route policy configuration:

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
  community "all-types" members "5000:[1-6][1-9][0-9]"
  community "all-normal" members "5000:[1-5][1-9][0-9]"
  as-path "Outside madeup paths" ".* 5001 .*
  as-path "Outside Internet paths" ".* 5002 .*
  policy-statement "RejectOutsideASPaths"
    entry 1
      from
        protocol bgpospf
      as-path "Outside madeup paths"
      exit
      action reject
      exit
    exit
    entry 2
      from
        protocol bgpospf
      as-path "Outside Internet paths"
      exit
      action reject
      exit
    exit
    entry 3
      from
        protocol ospf
      exit
      to
        protocol bgpospf
      exit
      action reject
      exit
    exit
    entry 4
      from
        protocol isis
      exit
      to
        protocol bgpospf
      exit
      action reject
      exit
    exit
  default-action accept
exit
policy-statement "aggregate-customer-peer-only"
```
entry 1
from
    community "all-customer-announce"
exit
    action accept
exit
exit
default-action reject
exit
exit

-----------------------------
A:ALA-B>config>router>policy-options#
Configuring Route Policy Components

Use the CLI syntax displayed below to configure:

- Creating a Route Policy on page 732
- Beginning the Policy Statement on page 731
- Configuring an Entry on page 734
- Configuring a Community List on page 735
- Configuring Damping on page 736
- Configuring a Prefix List on page 737
- Configuring PIM Join/Register Policies on page 738
BEGINNING THE POLICY STATEMENT

Use the following CLI syntax to begin a policy statement configuration. In order for a policy statement to be complete an entry must be specified (see Configuring an Entry on page 734).

CLI Syntax: config>router>policy-options
begin
    policy-statement name
description text

The following error message displays when the you try to modify a policy options command without entering begin first.

A:ALA-B>config>router>policy-options# policy-statement “allow all”
MINOR: CLI The policy-options must be in edit mode by calling begin before any changes can be made.

The following example displays policy statement configuration command usage. These commands are configured in the config>router context.

Example: config>router# policy-options
    policy-options# begin

There are no default policy statement options. All parameters must be explicitly configured.
Creating a Route Policy

To enter the mode to create or edit route policies, you must enter the `begin` keyword at the `config>router>policy-options` prompt. Other editing commands include:

- The `commit` command saves changes made to route policies during a session.
- The `abort` command discards changes that have been made to route policies during a session.

The following error message displays when you try to modify a policy options command without entering `begin` first.

```
A:ALA-B>config>router>policy-options# policy-statement "allow all"
MINOR: CLI The policy-options must be in edit mode by calling begin before any changes can
be made.

A:ALA-B>config>router>policy-options# info
#-------------------------------------------------
# Policy
#-------------------------------------------------

policy-options
begin
   policy-statement "allow all"
   description "General Policy"
 ... 
 exit
exit

-------------------------------------------------
A:ALA-B>config>router>policy-options#
```
Configuring a Default Action

Specifying a default action is optional. The default action controls those packets not matching any policy statement entries. If no default action is specified for the policy, then the action associated with the protocol to which the routing policy was applied is performed. The default action is applied only to those routes that do not match any policy entries.

A policy statement must include at least one entry (see Configuring an Entry on page 734).

To enter the mode to create or edit route policies, you must enter the `begin` keyword at the `config>router>policy-options` prompt. Other editing commands include:

- The `commit` command saves changes made to route policies during a session.
- The `abort` command discards changes that have been made to route policies during a session.

The following example displays the default action configuration:

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
policy-statement "1" 
default-action accept 
as-path add "test" 
community add "365" 
damping "flaptest" 
next-hop 10.10.10.104 
exit 
exit
----------------------------------------------
A:ALA-B>config>router>policy-options#
```
Configuring an Entry

An entry action must be specified. The other parameters in the entry action context are optional. Refer to the Route Policy Command Reference on page 745 for the commands and syntax.

The following example displays entry parameters and includes the default action parameters which were displayed in the previous section.

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
policy-statement "1"
   entry 1
to
   protocol bgp
   neighbor 10.10.10.104
exit
action accept
exit
exit
entry 2
from
   protocol ospf 1
exit
to
   protocol ospf
   neighbor 10.10.0.91
exit
action accept
exit
exit
default-action accept
   ...
exit
----------------------------------------------
A:ALA-B>config>router>policy-options#
policy-statement "exporttmsgrt"
   entry 1
from
   protocol vpn-leak
exit
action accept
exit
exit
entry 2
from
   protocol tms
exit
action accept
exit
exit
exit
commit
exit
```

Configuring a Community List

Community lists are composed of a group of destinations which share a common property. Community lists allow you to administer actions on a configured group instead of having to execute identical commands for each member.

The following example displays a community list configuration:

```
A:ALA-B(config)#router policy-options
----------------------------------------------
  community "eastern" members "100:200"
  community "western" members "100:300"
  community "northern" members "100:400"
  community "southern" members "100:500"
  community "headquarters" members "100:1000"
  policy-statement "1"
    entry 1
      to
        protocol bgp
        neighbor 10.10.10.104
        exit
        action accept
  . . .
----------------------------------------------
A:ALA-B(config)#
```
Configuring Damping

NOTES:

- For each damping profile, all parameters must be configured.
- The suppress value must be greater than the reuse value (see Figure 33 on page 727).
- Damping can be enabled in the config>router:bgp context on the BGP global, group, and neighbor levels. If damping is enabled, but route policy does not specify a damping profile, the default damping profile will be used. This profile is always present and consists of the following parameters:
  - half-life: 15 minutes
  - max-suppress: 60 minutes
  - suppress: 3000
  - reuse: 750

The following example displays a damping configuration:

```
*A:cses-A13>config>router>policy-options# info
----------------------------------------------
damping "damptest123"
  half-life 15
  max-suppress 60
  reuse 750
  suppress 1000
exit
----------------------------------------------
*A:cses-A13>config>router>policy-options#
```
Configuring a Prefix List

The following example displays a prefix list configuration:

```
A:ALA-B>config>router>policy-options# info
----------------------------------------------
prefix-list "western"
  prefix 10.10.0.1/32 exact
  prefix 10.10.0.2/32 exact
  prefix 10.10.0.3/32 exact
  prefix 10.10.0.4/32 exact
exit
damping "damptest123"
  half-life 15
  max-suppress 60
  reuse 750
exit
----------------------------------------------
A:ALA-B>config>router>policy-options#
```
Configuring PIM Join/Register Policies

Join policies are used in Protocol Independent Multicast (PIM) configurations to prevent the transportation of multicast traffic across a network and the dropping of packets at a scope at the edge of the network. PIM Join filters reduce the potential for denial of service (DoS) attacks and PIM state explosion—large numbers of Joins forwarded to each router on the RPT, resulting in memory consumption. See Importing PIM Join/Register Policies on page 75.

*,G or S,G is the information used to forward unicast or multicast packets.

- **group-address** matches the group in join/prune messages
  
group-address 229.55.150.208/32 exact

- **source-address** matches the source in join/prune messages
  
source-address 192.168.0.0/16 longer

- **interface** matches any join message received on the specified interface
  
interface port 1/1/1

- **neighbor** matches any join message received from the specified neighbor
  
neighbor 1.1.1.1

The following configuration example will not allow join messages for group 229.50.50.208/32 and source 192.168.0.0/16 but allows other join messages.

Configuring policy-statement

```
A:ALA-B>config>router# policy-options
A:ALA-B>config>router>policy-options# begin
A:ALA-B>config>router>policy-options# policy-statement foo
A:ALA-B>config>router>policy-options>policy-statement$ entry 10
A:ALA-B>config>router>policy-options>policy-statement>entry$ from
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ group-address
229.50.50.208/32
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ source-address
192.168.0.0
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ exit
A:ALA-B>config>router>policy-options>policy-statement>entry$ action reject
A:ALA-B>config>router>policy-options>policy-statement# exit
```

The following configuration example allows registers for *, 224.0.0.0/8.

```
A:ALA-B>config>router>policy-options# policy-statement reg-pol
A:ALA-B>config>router>policy-options>policy-statement$ entry 10
A:ALA-B>config>router>policy-options>policy-statement>entry$ from
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ group-address
224.0.0.0/8
A:ALA-B>config>router>policy-options>policy-statement>entry# action accept
A:ALA-B>config>router>policy-options>policy-statement>entry# exit
A:ALA-B>config>router>policy-options>policy-statement# exit
```
A:ALA-B>config>router>policy-options# info
---------------------------------------------------------
...
    policy-statement "foo"
       entry 10
          from
             group-address "229.50.50.208/32"
             source-address 192.168.0.0
          exit
             action reject
          exit
          exit
          exit
    policy-statement "reg-pol"
       entry 10
          from
             group-address "224.0.0.0/8"
          exit
             action accept
          exit
          exit
          exit
...
---------------------------------------------------------
A:ALA-B>config>router>policy-options#
Configuring Bootstrap Message Import and Export Policies

Bootstrap import and export policies are used to control the flow of bootstrap messages to and from the RP.

The following configuration example specifies that no BSR messages received or sent out of interface port 1/1/1.

```
A:ALA-B>config>router>policy-options# policy-statement pim-import
A:ALA-B>config>router>policy-options>policy-statement$ entry 10
A:ALA-B>config>router>policy-options>policy-statement$ from
A:ALA-B>config>router>policy-options>policy-statement>from$ interface port 1/1/1
A:ALA-B>config>router>policy-options>policy-statement>from$ exit
A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
A:ALA-B>config>router>policy-options>policy-statement>entry# exit
A:ALA-B>config>router>policy-options>policy-statement# exit

A:ALA-B>config>router>policy-options# policy-statement pim-export
A:ALA-B>config>router>policy-options>policy-statement$ entry 10
A:ALA-B>config>router>policy-options>policy-statement$ to
A:ALA-B>config>router>policy-options>policy-statement>to$ interface port 1/1/1
A:ALA-B>config>router>policy-options>policy-statement>to$ exit
A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
A:ALA-B>config>router>policy-options>policy-statement>entry# exit
A:ALA-B>config>router>policy-options>policy-statement# exit

A:ALA-B>configure router pim rp bootstrap-import pim-import
A:ALA-B>configure router pim rp bootstrap-export pim-export
```
Route Policy Configuration Management Tasks

This section discusses the following route policy configuration management tasks:

- Editing Policy Statements and Parameters on page 741
- Deleting an Entry on page 743
- Deleting a Policy Statement on page 743

Editing Policy Statements and Parameters

Route policy statements can be edited to modify, add, or delete parameters. To enter the mode to edit route policies, you must enter the `begin` keyword at the `config>router> policy-options` prompt. Other editing commands include:

- The `commit` command saves changes made to route policies during a session.
- The `abort` command discards changes that have been made to route policies during a session.

The following example displays a changed configuration:

```
A:ALA-B>config>router>policy-options>policy-statement# info
----------------------------------------------
description "Level 1"
entry 1
to
    protocol bgp
    neighbor 10.10.10.104
exit
action accept
exit
exit
entry 2
from
    protocol ospf
exit
to
    protocol ospf
    neighbor 10.10.0.91
exit
action accept
exit
exit
entry 4
description "new entry"
from
    protocol isis
    area 0.0.0.20
exit
action reject
```
exit
default-action accept
    as-path add "test"
    community add "369"
    damping "flapper"
    next-hop 10.10.10.104
exit
---------------------------------------------------
Deleting an Entry

Use the following CLI syntax to delete a policy statement entry:

**CLI Syntax:**
```
cfg-router-policy-options
  begin
  commit
  abort
  policy-statement name
  no entry entry-id
```

The following example displays the commands required to delete a policy statement entry.

**Example:**
```
config>router>policy-options# begin
policy-options# policy-statement "1"
policy-options>policy-statement# no entry 4
policy-options>policy-statement# commit
```
Route Policy Command Reference

Command Hierarchies

- Route Policy Configuration Commands on page 745
- Show Commands on page 748

Route Policy Configuration Commands

```plaintext
config
  - [no] router
    - [no] triggered-policy
    - [no] policy-options
      - begin
      - commit
      - abort
      - as-path (policy options) name {regular-expression | null}
      - no as-path (policy options) name
      - community name members comm-id [comm-id ... (up to 15 max)]
      - no community name [members comm-id]
      - [no] damping name
        - half-life minutes
        - no half-life
        - max-suppress minutes
        - no max-suppress
        - reuse integer
        - no reuse
        - suppress integer
        - no suppress
      - [no] exclusive-lock-time seconds
      - [no] policy-statement name
        - default-action {accept | next-entry | next-policy | reject}
        - no default-action
          - as-path [add | replace] name
          - no as-path
          - as-path-prepend as-number [ repeat]
          - no as-path-prepend
          - community { {add name [remove name]} | {remove name [add name]} } | {replace name} }
          - no community
          - damping {name | none}
          - no damping
          - local-preference local-preference
          - no local-preference
          - metric {add |subtract} metric
          - metric set [igp|metric-value]
          - no metric
          - multicast-redirection [fwd-service service-id] ip-int-name
```
— no multicast-redirection
— next-hop ip-address
— no next-hop
— [no] next-hop-self
— origin {igp | egp | incomplete}
— no origin
— preference preference
— no preference
— tag hex-string
— no tag
— type {type}
— no type
— description description-string
— no description
— [no] entry entry-id
— action {accept | next-entry | next-policy | reject}
— no action
  — as-path {add | replace} name
  — no as-path
  — as-path-prepend as-number [ repeat]
  — no as-path-prepend
  — community { {add name | remove name} | {remove name
    add name} | {replace name}}
  — no community
  — damping {name | none}
  — no damping
  — fc fc [priority {low | high}]
  — no fc
  — local-preference local-preference
  — no local-preference
  — metric {set {igp | number 1} | {add | subtract} number2}
  — no metric
  — next-hop ip-address
  — no next-hop
  — [no] next-hop-self
  — [no] next-hop-self
  — origin {igp | egp | incomplete}
  — no origin
  — preference preference
  — no preference
  — tag tag
  — no tag
  — type {type}
  — no type
— description description-string
— no description
— [no] from
  — area area-id
  — no area
  — as-path name
  — no as-path
  — community name
  — no community
  — [no] external
— family [ipv4] [mcast-ipv4] [vpn-ipv4] [l2-vpn] [mvpn-ipv4] [ndt-safi] [flow-ipv4] [route-target] [mcast-vpn-ipv4]
— no family
— group-address prefix-list-name
— no group-address
— host-ip prefix-list-name
— no host-ip
— interface interface-name
— no interface
— level {1 | 2}
— no level
— neighbor {ip-address | prefix-list name}
— no neighbor
— origin {igp | egp | incomplete | any}
— no origin
— prefix-list name [name...(up to 5 max)]
— no prefix-list
— protocol protocol [all | instance instance]
— no protocol
— source-address ip-address
— no source-address
— state state
— no state
— tag tag
— no tag
— type type
— no type

— [no] to
— level {1 | 2}
— no level
— neighbor {ip-address | prefix-list name}
— no neighbor
— [no] prefix-list name [name...(up to 5 max)]
— protocol protocol
— no protocol
config
  — [no] router
  — [no] policy-options
       — [no] prefix-list name
            — prefix ip-prefix/prefix-length [exact | longer | through length | prefix-length-range length1-length2]
            — no prefix [ipv-prefix/prefix-length] [exact | longer | through length | prefix-length-range length1-length2]

Show Commands

show
  — router router-name
       — policy [name | damping | prefix-list name | as-path name | community name | admin]
Route Policy Command Reference

Generic Commands

abort

Syntax  abort
Context config>router>policy-options
This command is required to discard changes made to a route policy.
Default none

begin

Syntax  begin
Context config>router>policy-options
Description This command is required in order to enter the mode to create or edit route policies.
Default none

commit

Syntax  commit
Context config>router>policy-options
Description This command is required to save changes made to a route policy.
Default none
Generic Commands

description

Syntax  description string
        no description

Context  config>router-policy-options-policy-statement
         config>router-policy-options-policy-statement>entry

Description  This command creates a text description which is stored in the configuration file to help identify the content of the entity.
              The no form of the command removes the string from the configuration.

Default  none

Parameters  string — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
Route Policy Options

as-path (policy options)

**Syntax**

```
as-path name {reg-exp | null}
no as-path name
```

**Context**

```
config>router>policy-options
```

**Description**

This command creates a route policy AS path regular expression statement to use in route policy entries. The **no** form of the command deletes the AS path regular expression statement.

**Default**

No AS path regular expression statement is defined.

**Parameters**

- **name** — The AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

- **reg-exp** — The AS path regular expression. Allowed values are any string up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

- **null** — The AS path expressed as an empty regular expression string.

community

**Syntax**

```
community name members comm-id [comm-id...up to 15 max]
no community name [members comm-id ]
```

**Context**

```
config>router>policy-options
```

**Description**

This command creates a route policy community list to use in route policy entries. The **no** form of the command deletes the community list or the provided community ID.

**Default**

**no community** — No community names or members are specified.

**Parameters**

- **name** — The community list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

- **comm-id** — The community ID. Note that up to 15 community ID strings can be specified up to a total maximum of 72 characters.

**Values**

- 72 chars max
- 2byte-asnumber:comm-val | reg-ex | ext-comm | well-known-comm
- 2byte-asnumber 0..65535
A community ID can be specified in different forms:

- **as-num:comm.-value** — The as-num is the Autonomous System Number (ASN)
  
  **Values**
  
  - as-num: 1 — 65535
  - comm-value: 0 — 65535

- **type {target | origin} :as-num:comm.-value** — The keywords target or origin denote the community as an extended community of type route target or route origin respectively. The as-num and comm.-value allow the same values as described above for regular community values.

- **reg-ex1 reg-ex2** — A regular expression string. Allowed values are any string up to 63 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

- **well-known-comm** — keywords null, no-export, no-export-subconfed, no-advertise

### exclusive-lock-time

**Syntax**

```
exclusive-lock-time seconds
no exclusive-lock
```

**Context**

config>router>policy-options

**Description**

This command specifies the inactivity timer for the exclusive lock time for policy editing. When a session is idle for greater than this time, the lock is removed and the configuration changes are aborted.

**Default**

300 seconds

**Parameters**

- **seconds** — Specifies the duration the session with exclusive lock may be inactive.

  **Values**

  - Values 1 - 3600

### policy-options

**Syntax**

```
[no] policy-options
```

**Context**

config>router

**Description**

This command enables the context to configure route policies. Route policies are applied to the routing protocol.
The `no` form of the command deletes the route policy configuration.

**Default**

`none`

**triggered-policy**

**Syntax**

`[no] triggered-policy`

**Context**

`config>router`

**Description**

This command triggers route policy re-evaluation. By default, when a change is made to a policy in the `config router policy options` context and then committed, the change is effective immediately. There may be circumstances when the changes should or must be delayed; for example, if a policy change is implemented that would effect every BGP peer on a router, the consequences could be dramatic. It is more effective to control changes on a peer by peer basis.

If the `triggered-policy` command is enabled, and a given peer is established, and you want the peer to remain up, then, in order for a change to a route policy to take effect, a `clear` command with the `soft` or `soft-inbound` option must be used. In other words, when a `triggered-policy` is enabled, any routine policy change or policy assignment change within the protocol will not take effect until the protocol is reset or a clear command is issued to re-evaluate route policies; for example, `clear router bgp neighbor x.x.x.x soft`. This keeps the peer up and the change made to a route policy is applied only to that peer, or group of peers.

**Default**

Non-dynamic route policy is disabled.
Route Policy Damping Commands

damping

Syntax  [no] damping name

Context  config>router>policy-options

Description  This command creates a context to configure a route damping profile to use in route policy entries. The no form of the command deletes the named route damping profile.

Default  No damping profiles are defined.

Parameters  name — The damping profile name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

half-life

Syntax  half-life minutes
no half-life

Context  config>router>policy-options>damping

Description  This command configures the half-life parameter for the route damping profile. The half life value is the time, expressed in minutes, required for a route to remain stable in order for the Figure of Merit (FoM) value to be reduced by one half; for example, if the half life value is 6 (minutes) and the route remains stable for 6 minutes, then the new FoM value is 3 (minutes). After another 3 minutes pass and the route remains stable, the new FoM value is 1.5 (minutes). When the FoM value falls below the reuse threshold, the route is once again considered valid and can be reused or included in route advertisements.

The no form of the command removes the half life parameter from the damping profile.

Default  No half life value is specified. The half life value must be explicitly configured.

Parameters  minutes — The half life in minutes expressed as a decimal integer.

Values  1 — 45
max-suppress

Syntax  max-suppress minutes
       no max-suppress

Context config>router>policy-options>damping

Description This command configures the maximum suppression parameter for the route damping profile.
This value indicates the maximum time, expressed in minutes, that a route can remain suppressed.
The no form of the command removes the maximum suppression parameter from the damping profile.

Default No maximum suppression time is configured.

Parameters minutes — The maximum suppression time, in minutes, expressed as a decimal integer.

   Values 1 — 720

reuse

Syntax  reuse integer
       no reuse

Context config>router>policy-options>damping

Description This command configures the reuse parameter for the route damping profile.
When the Figure of Merit (FoM) value falls below the reuse threshold, the route is once again considered valid and can be reused or included in route advertisements.
The no form of the command removes the reuse parameter from the damping profile.

Default No reuse parameter is configured.

Parameters integer — The reuse value expressed as a decimal integer.

   Values 1 — 20000
### suppress

**Syntax**

```plaintext
suppress integer
no suppress
```

**Context**

config>router>policy-options>damping

**Description**

This command configures the suppression parameter for the route policy damping profile.

A route is suppressed when it has flapped frequently enough to increase the Figure of Merit (FoM) value to exceed the `suppress` threshold limit. When the FoM value exceeds the `suppress` threshold limit, the route is removed from the route table or inclusion in advertisements.

The `no` form of the command removes the suppress parameter from the damping profile.

**Default**

No suppress parameter is configured.

**Parameters**

`integer` — The suppress value expressed as a decimal integer.

**Values**

1 — 20000
Route Policy Prefix Commands

prefix-list

Syntax  
[no] prefix-list name

Context  
config>router>policy-options

Description  
This command creates a context to configure a prefix list to use in route policy entries. The no form of the command deletes the named prefix list.

Default  
none

Parameters  
name — The prefix list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

prefix

Syntax  
[no] prefix ip-prefix/prefix-length { [exact | longer | through length ] } [prefix-length-range length1-length2 ]

[no] prefix [ip-prefix/prefix-length] [exact | longer | through length ] [prefix-length-range length1-length2 ]

Context  
config>router>policy-options>prefix-list

Description  
This command creates a prefix entry in the route policy prefix list. The no form of the command deletes the prefix entry from the prefix list.

Parameters  
ip-prefix — The IP prefix for prefix list entry in dotted decimal notation.

Values  
ipv4-prefix: a.b.c.d (host bits must be 0)
ipv4-prefix-length: 0 — 32

exact — Specifies the prefix list entry only matches the route with the specified ip-prefix and prefix mask (length) values.

longer — Specifies the prefix list entry matches any route that matches the specified ip-prefix and prefix mask length values equal to or greater than the specified mask.

through length — Specifies the prefix list entry matches any route that matches the specified ip-prefix and has a prefix length between the specified length values inclusive.

Values  
0 — 32

prefix-length-range length1 - length2 — Specifies a route must match the most significant bits and have a prefix length with the given range. The range is inclusive of start and end values.

Values  
0 — 32, length2 > length1
Route Policy Entry Match Commands

entry

Syntax
entry entry-id
no entry

Context
config>router>policy-options>policy-statement

Description
This command creates the context to edit route policy entries within the route policy statement. Multiple entries can be created using unique entries. The router exits the filter when the first match is found and executes the action specified. For this reason, entries must be sequenced correctly from most to least explicit.

An entry does not require matching criteria defined (in which case, everything matches) but must have at least define an action in order to be considered complete. Entries without an action are considered incomplete and will be rendered inactive.

The no form of the command removes the specified entry from the route policy statement.

Default
none

Parameters
entry-id — The entry ID expressed as a decimal integer. An entry-id uniquely identifies match criteria and the corresponding action. It is recommended that multiple entries be given entry-ids in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

Values
1 — 4294967295

area

Syntax
area area-id
no area

Context
config>router>policy-options>policy-statement>entry>from

Description
This command configures an OSPF area as a route policy match criterion. This match criterion is only used in export policies.

All OSPF routes (internal and external) are matched using this criterion if the best path for the route is by the specified area.

The no form of the command removes the OSPF area match criterion.

Default
none

Parameters
area-id — The OSPF area ID expressed in dotted decimal notation or as a 32-bit decimal integer.

Values
0.0.0.0 — 255.255.255.255 (dotted decimal), 0 — 4294967295 (decimal)
as-path

Syntax  as-path name
       no as-path

Context  config>router>policy-options>policy-statement>entry>from

Description  This command configures an AS path regular expression statement as a match criterion for the route policy entry.

If no AS path criterion is specified, any AS path is considered to match.

AS path regular expression statements are configured at the global route policy level (config>router>policy-options>as-path name).

The no form of the command removes the AS path regular expression statement as a match criterion.

Default  no as-path — Matches any AS path.

Parameters  name — Specifies an existing name. The AS path regular expression name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

community

Syntax  community name
       no community

Context  config>router>policy-options>policy-statement>entry>from

Description  This command configures a community list as a match criterion for the route policy entry.

If no community list is specified, any community is considered a match.

The no form of the command removes the community list match criterion.

Default  no community — Matches any community.

Parameters  name — The community list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The name specified must already be defined.

from

Syntax  [no] from

Context  config>router>policy-options>policy-statement>entry

Description  This command creates the context to configure policy match criteria based on a route’s source or the protocol from which the route is received.
Route Policy Entry Match Commands

If no condition is specified, all route sources are considered to match.
The `no` form of the command deletes the source match criteria for the route policy statement entry.

**external**

**Syntax**

`[no] external`

**Context**

`config>router>policy-options>policy-statement>entry>from`

**Description**

This command specifies the external route matching criteria for the entry.

**Default**

`no external`

**family**

**Syntax**

`family [ipv4] [mcast-ipv4] [vpn-ipv4] [l2- vpn] [mvpn-ipv4] [mdt-safi] [flow-ipv4] [route-target] [mcast- vpn-ipv4] no family`

**Context**

`config>router>policy-options>policy-statement>entry>from`

**Description**

This command specifies address families as matching conditions.

**Parameters**

- `ipv4` — Specifies IPv4 routing information.
- `mcast-ipv4` — Specifies multicast IPv4 routing information.
- `vpn-ipv4` — Specifies IPv4 VPN routing information.
- `l2-vpn` — Exchanges Layer 2 VPN information.
- `mvpn-ipv4` — Exchanges Multicast VPN related information
- `mdt-safi` — Exchange Multicast VPN (MDT-SAFI) related information
- `flow-ipv4` — Exchanges IPv4 flowspec routes belonging to AFI 1 and SAFI 133
- `route-target` — Specifies to use route targets to be advertised to the peers if ORF is enabled for this peer group
- `mcast-vpn-ipv4` — Exchanges Multicast Routes in VPN using SAFI 129.
**group-address**

**Syntax**  
```text
    group-address prefix-list-name
no group-address
```

**Context**  
```
config>router>policy-options>policy-statement>entry>from
```

**Description**  
This command specifies the multicast group-address prefix list containing multicast group-addresses that are imbedded in the join or prune packet as a filter criterion. The prefix list must be configured prior to entering this command. Prefix lists are configured in the `config>router>policy-options>prefix-list` context.

The `no` form of the command removes the criterion from the configuration.

**Default**  
`no group-address`

**Parameters**  
- `prefix-list-name` — The prefix-list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

  The `prefix-list-name` is defined in the `config>router>policy-options>prefix-list` context.

**host-ip**

**Syntax**  
```text
    host-ip prefix-list-name
```

**Context**  
```
config>router>policy-options>policy-statement>entry>from
```

**Description**  
This command specifies a prefix list host IP address as a match criterion for the route policy-statement entry.

**Default**  
`no host-ip`

**Parameters**  
- `prefix-list-name` — The prefix-list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

  The `prefix-list-name` is defined in the `config>router>policy-options>prefix-list` context.

**interface**

**Syntax**  
```text
    interface interface-name
no interface
```

**Context**  
```
config>router>policy-options>policy-statement>entry>from
```

**Description**  
This command specifies the router interface, specified either by name or address, as a filter criterion.

The `no` form of the command removes the criterion from the configuration.

**Default**  
`no interface`

**Parameters**  
- `ip-int-name` — Specify the name of the interface as a match criterion for this entry. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
level

Syntax  level {1 | 2}
        no level

Context  config>router>policy-options>policy-statement>entry>from
         config>router>policy-options>policy-statement>entry>to

Description  This command specifies the ISIS route level as a match criterion for the entry.

Default  no level

Parameters  1 | 2 — Matches the IS-IS route learned from level 1 or level 2.

neighbor

Syntax  neighbor {ip-address | prefix-list name}
        no neighbor

Context  config>router>policy-options>policy-statement>entry>to
         config>router>policy-options>policy-statement>entry>from

Description  This command specifies the neighbor address as found in the source address of the actual join and prune message as a filter criterion. If no neighbor is specified, any neighbor is considered a match. The no form of the of the command removes the neighbor IP match criterion from the configuration.

Default  no neighbor — Matches any neighbor.

Parameters  ip-addr — The neighbor IP address in dotted decimal notation.
            Values  ipv4-address:  a.b.c.d

            prefix-list name — The prefix-list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

            The name specified must already be defined.

origin

Syntax  origin {igp | egp | incomplete | any | aaa | dhcp | lubd}
        no origin

Context  config>router>policy-options>policy-statement>entry>from

Description  This command will configure a match criteria for the origin attribute. Originally, the origin attribute was applicable only to BGP as a mandatory well-known BGP attribute.

            The functionality of the origin attribute has expanded to subscriber-management routes (/32 IPv4 host and IPv6 PD wan-host routes). Each subscriber-management route will internally (local to the node) by default carry the origin attribute with one of the three new values (aaa, dhcp and lubd). The value of the attribute will
Route Policies

depend on the origin of the subscriber-management route. The aaa, dhcp or ludb values will never be carried in BGP updates as part of the BGP origin attribute or be otherwise visible within the BGP process.

This introduction of the three new values for the origin attribute in the subscriber-management routes will allow customized advertisement of the subscriber-management routes via routing policy.

**Default**

**no origin** — Matches any BGP origin attribute

**Parameters**

**igp** — Configures matching path information originating within the local AS.

**egp** — Configures matching path information originating in another AS.

**incomplete** — Configures matching path information learned by another method.

**any** — Specifies to ignore this criteria.

**aaa** — IPv4

subscriber-management /32 host routes that are originated via Radius framed-ip-address VSA other than 255.255.255.254. The 255.255.255.254 returned by the Radius indicates that the BNG (NAS) should assign an IP address from its own pool.

IPv6

subscriber-management routes that are originated through framed-ipv6-prefix (SLAAC), delegated-ipv6-prefix (IA_PD) or alc-ipv6-address (IA_NA) Radius attributes. This is valid for IPoE and PPPoE type host.

**dhcp** — IPv4

subscriber-management /32 host routes that are originated via DHCP server (local or remote) and also Radius framed-ip-address=255.255.255.254 (RFC 2865).

IPv6

subscriber-management routes that are assigned via local DHCPv6 server pools whose name is obtained through Alc-Delegated-IPv6-Pool (PD pool) and Framed-IPv6-Pool (NA pool) Radius attributes. This is valid for IPoE and PPPoE type hosts.

In addition, for IPoEv6 only, the pool name can be also obtained via ipv6-delegated-prefix-pool (PD pool) and ipv6-wan-address-pool (NA pool) from LUDB.

**ludb** — IPv4

subscriber-management /32 host routes that are originated via LUDB. This should also cover Radius fallback category (Radius falls back to system-defaults or to LUDB).

IPv6

subscriber-management routes obtained from LUDB via ipv6-address (IA_NA) or ipv6-prefix (IA_PD). This is supported only for IPoE.
policy-statement

Syntax  
[no] policy-statement name

Context  
config>router>policy-options

Description  
This command creates the context to configure a route policy statement.

Route policy statements control the flow of routing information to and from a specific protocol, set of protocols, or to a specific BGP neighbor.

The policy-statement is a logical grouping of match and action criteria. A single policy-statement can affect routing in one or more protocols and/or one or more protocols peers/neighbors. A single policy-statement can also affect both the import and export of routing information.

The no form of the command deletes the policy statement.

Default  
no policy-statement — No route policy statements are defined.

Parameters  
name — The route policy statement name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

prefix-list

Syntax  
prefix-list name [name...up to 5 max]  
no prefix-list

Context  
config>router>policy-options>policy-statement>entry>from  
config>router>policy-options>policy-statement>entry>to

Description  
This command configures a prefix list as a match criterion for a route policy statement entry.

If no prefix list is specified, any network prefix is considered a match.

The prefix lists specify the network prefix (this includes the prefix and length) a specific policy entry applies.

A maximum of five prefix names can be specified.

The no form of the command removes the prefix list match criterion.

Default  
no prefix-list — Matches any network prefix.

Parameters  
name — The prefix list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.
**protocol**

**Syntax**

```
protocol {protocol} [all | instance instance]
no protocol
```

**Context**

```
config>router>policy-options>policy-statement>entry>to
config>router>policy-options>policy-statement>entry>from
```

**Description**

This command configures a routing protocol as a match criterion for a route policy statement entry. This command is used for both import and export policies depending how it is used.

If no protocol criterion is specified, any protocol is considered a match.

The `no` form of the command removes the protocol match criterion.

**Default**

`no protocol` — Matches any protocol.

**Parameters**

`protocol` — The protocol name to match on.

- **Values**
  - `direct`, `static`, `bgp`, `isis`, `ospf`, `rip`, `aggregate`, `bgp-vpn`, `igmp`, `pim`, `ospf3`, `ldp`, `sub-mgmt`, `mld`, `managed`, `vpn-leak`, `tms`, `nat`, `periodic`, `ipsec`, `mpls`
  - `instance` — The OSPF or IS-IS instance.
  - **Values**
    - `1 — 31`
    - `all` — OSPF- or ISIS-only keyword.

**source-address**

**Syntax**

```
source-address ip-address
no source-address
```

**Context**

```
config>router>policy-options>policy-statement>entry>from
```

**Description**

This command specifies the source address that is embedded in the join or prune packet as a filter criterion.

The `no` form of the command removes the criterion from the configuration.

**Default**

`none`

**Description**

This command specifies a multicast data source address as a match criterion for this entry.

**Parameters**

`ip-address` — The IP prefix for the IP match criterion in dotted decimal notation.
Route Policy Entry Match Commands

**state**

**Syntax**  
state state  
no state

**Context**  
config>router>policy-options>policy-statement>entry>from

**Description**  
This command will configure a match criteria on the state attribute. The state attribute carries the state of an SRRP instance and it can be applied to:

- subscriber-interface routes
- subscriber-management routes (/32 IPv4 and IPv6 PD wan-host)
- managed-routes (applicable only to IPv4).

Based on the state attribute of the route we can manipulate the route advertisement into the network.

We can enable or disable (in case there is no SRRP running) tracking of SRRP state by routes.

This is done on a per subscriber-interface route basis, where a subscriber-interface route is tracking a single SRRP instance state (SRRP instance might be in a Fate Sharing Group).

For subscriber-management and managed-routes, tracking is enabled per group interface under which SRRP is enabled.

**Default**  
none

**Description**  
This command specifies a multicast data source address as a match criterion for this entry.

**Parameters**  
- srrp-master — Track routes with the state attribute carrying srrp-master state.
- srrp-non-master — Track routes with the state attribute carrying srrp-non-master state.
- ipsec-master-with-peer — Track routes with the state attribute carrying ipsec-master-with-peer state.
- ipsec-non-master — Track routes with the state attribute carrying ipsec-non-master state.
- ipsec-master-without-peer — Track routes with the state attribute carrying ipsec-master-without-peer state.

**tag**

**Syntax**  
tag tag  
no tag

**Context**  
config>router>policy-options>policy-statement>entry>from

**Description**  
This command matches the tag value on routes of type static, periodic as well as the tag field on routes learned through an external LSA.

The no form of the command removes the tag field match criterion.

**Default**  
no tag — Matches any external LSA tag field.

**Parameters**  
tag — Matches a specific external LSA tag field.

**Values**  
- no-tag, 1 — 4294967295
**to**

**Syntax**

[no] to

**Context**

config>router>policy-options>policy-statement>entry

**Description**

This command creates the context to configure export policy match criteria based on a route’s destination or the protocol into which the route is being advertised.

If no condition is specified, all route destinations are considered to match.

The `to` command context only applies to export policies. If it is used for an import policy, match criteria is ignored.

The `no` form of the command deletes export match criteria for the route policy statement entry.

**type**

**Syntax**

type {1 | 2}

no type

**Context**

config>router>policy-options>policy-statement>entry>from

**Description**

This command configures an OSPF type metric as a match criterion in the route policy statement entry.

If no type is specified, any OSPF type is considered a match.

The `no` form of the command removes the OSPF type match criterion.

**Parameters**

1 — Matches OSPF routes with type 1 LSAs.

2 — Matches OSPF routes with type 2 LSAs.
Route Policy Action Commands

action

Syntax  action {accept | next-entry | next-policy | reject}
        no action

Context  config>router>policy-options>policy-statement>entry

Description  This command creates the context to configure actions to take for routes matching a route policy statement entry.
              This command is required and must be entered for the entry to be active.
              Any route policy entry without the action command will be considered incomplete and will be inactive.
              The no form of the command deletes the action context from the entry.

Default  no action — No action is defined.

Parameters  accept — Specifies routes matching the entry match criteria will be accepted and propagated.
             next-entry — Specifies that the actions specified would be made to the route attributes and then policy evaluation would continue with next policy entry (if any others are specified).
             next-policy — Specifies that the actions specified would be made to the route attributes and then policy evaluation would continue with next route policy (if any others are specified).
             reject — Specifies routes matching the entry match criteria would be rejected.

as-path

Syntax  as-path {add | replace} name
        no as-path

Context  config>router>policy-options>policy-statement>default-action
         config>router>policy-options>policy-statement>entry>action

Description  This command assigns a BGP AS path list to routes matching the route policy statement entry.
              If no AS path list is specified, the AS path attribute is not changed.
              The no form of the command disables the AS path list editing action from the route policy entry.

Default  no as-path — The AS path attribute is not changed.

Parameters  add — Specifies that the AS path list is to be prepended to an existing AS list.
             replace — Specifies AS path list replaces any existing as path attribute.
**Route Policies**

name — The AS path list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

The *name* specified must already be defined.

**as-path-prepend**

**Syntax**

```
as-path-prepend as-num [repeat]
no as-path-prepend
```

**Context**

```
config>router>policy-options>policy-statement>default-action
cfg>config>router>policy-options>policy-statement>entry>action
```

**Description**

The command prepends a BGP AS number once or numerous times to the AS path attribute of routes matching the route policy statement entry.

If an AS number is not configured, the AS path is not changed.

If the optional *number* is specified, then the AS number is prepended as many times as indicated by the number.

The *no* form of the command disables the AS path prepend action from the route policy entry.

**Default**

`no as-path-prepend` — no AS number prepending configured.

**Parameters**

- **as-num** — The AS number to prepend expressed as a decimal integer.
  - **Values**
    - 1 — 4294967295
  - **repeat** — The number of times to prepend the specified AS number expressed as a decimal integer.
  - **Values**
    - 1 — 50

**community**

**Syntax**

```
community {{add name [remove name]} | {remove name [add name]} | {replace name}}
no community
```

**Context**

```
config>router>policy-options>policy-statement>default-action
cfg>config>router>policy-options>policy-statement>entry>action
```

**Description**

This command adds or removes a BGP community list to or from routes matching the route policy statement entry.

If no community list is specified, the community path attribute is not changed.

The community list changes the community path attribute according to the *add* and *remove* keywords.

The *no* form of the command disables the action to edit the community path attribute for the route policy entry.

**Default**

`no community` — The community path attribute is not changed.
Parameters

- **add** — The specified community list is added to any existing list of communities.
- **remove** — The specified community list is removed from the existing list of communities.
- **replace** — The specified community list replaces any existing community attribute.

- **name** — The community list name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

### damping

**Syntax**

```
damping {name | none}
```

**Context**

```
config>router>policy-options>policy-statement >default-action
config>router>policy-options>policy-statement>entry>action
```

**Description**

This command configures a damping profile used for routes matching the route policy statement entry. If no damping criteria is specified, the default damping profile is used. The **no** form of the command removes the damping profile associated with the route policy entry.

**Default**

```
no damping — Use the default damping profile.
```

**Parameters**

- **name** — The damping profile name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

  The **name** specified must already be defined.

- **none** — Disables route damping for the route policy.

### fc

**Syntax**

```
fc fc [priority {low | high}]
```

**Context**

```
config>router>policy-options>policy-statement>entry>action
```

**Description**

This command associates a forwarding-class and optionally priority with the routes matched by a route policy entry. The command takes effect when the action of the route policy entry is accept, next-entry or next-policy. It has no effect except in route policies applied as VRF import policies, BGP import policies or RIP import policies.

The **no** form of the command removes the QoS association of the routes matched by the route policy entry.

**Default**

```
no fc
```
Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>fc</strong></td>
<td>Specify the name of one of the predefined forwarding classes in the system.</td>
</tr>
<tr>
<td><strong>Values</strong></td>
<td>be, l2, af, l1, h2, ef, h1, nc</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>none (no QoS information is associated with matched routes)</td>
</tr>
</tbody>
</table>

**priority**

- **Values**
  - **low** — Setting the enqueuing parameter to high for a packet increases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing. Once the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.
  - **high** — Setting the enqueuing parameter to low for a packet decreases the likelihood of enqueuing the packet when the ingress queue is congested. Ingress enqueuing priority only affects ingress SAP queuing, once the packet is placed in a buffer on the ingress queue, the significance of the enqueuing priority is lost.

- **Default** low

**default-action**

- **Syntax**
  - default-action {accept | next-entry | next-policy | reject}
  - no default-action

- **Context**
  - config>router>policy-options>policy-statement

- **Description**
  - This command enables the context to configure actions for routes that do not match any route policy statement entries when the accept parameter is specified.
  - The default action clause can be set to all available action states including: accept, reject, next-entry and next-policy. If the action states accept or reject then the policy evaluation terminates and the appropriate result is returned.
  - If a default action is defined and no match(es) occurred with the entries in the policy then the default action clause is used.
  - If a default action is defined and one or more matches occurred with the entries of the policy then the default action is not used.
  - The no form of the command deletes the default-action context for the policy statement.

- **Default** no default-action — No default action is specified.

- **Parameters**
  - **accept** — Specifies routes matching the entry match criteria will be accepted and propagated.
  - **next-entry** — Specifies that the actions specified would be made to the route attributes and then policy evaluation would continue with next policy entry (if any others are specified).
  - **next-policy** — Specifies that the actions specified would be made to the route attributes and then policy evaluation would continue with next route policy (if any others are specified).
  - **reject** — Specifies routes matching the entry match criteria would be rejected.
local-preference

Syntax  
local-preference preference  
no local-preference

Context  
config>router>policy-options>policy-statement>default-action  
config>router>policy-options>policy-statement>entry

Description  
This command assigns a BGP local preference to routes matching a route policy statement entry.  
If no local preference is specified, the BGP configured local preference is used.  
The no form of the command disables assigning a local preference in the route policy entry.

Default  
No local-preference — BGP default preference is assigned.

Parameters  
preference — The local preference expressed as a decimal integer.

Values  
0 — 4294967295

metric

Syntax  
metric {add|subtract} metric  
metric set [igp|metric-value]  
no metric

Context  
config>router>policy-options>policy-statement>default-action  
config>router>policy-options>policy-statement>entry>action

Description  
In a BGP import or export policy, this command assigns a MED value to routes matched by the policy statement entry. The MED value may be set to a fixed value (overriding the received value), set to the routing table cost of the route used to resolve the NEXT_HOP of the BGP route (igp option), or modified by adding or subtracting a fixed value offset.  
The no form of the command removes the MED attribute from the matched routes.

Default  
no metric — Uses the configured metric (if defined) or do not advertise a metric.

Parameters  
add — Specified integer is added to any existing metric. If the result of the addition results in a number greater than 4294967295, the value 4294967295 is used.

subtract — Specified integer is subtracted from any existing metric. If the result of the subtraction results in a number less than 0, the value of 0 is used.

set — Specified integer replaces any existing metric.

igp — Sets the MED value to the routing table cost of the route used to resolve the NEXT_HOP of the BGP route.

metric — The metric modifier expressed as a decimal integer.

Values  
0 — 4294967295
multicast-redirection

**Syntax**
```
multicast-redirection [fwd-service service-id] ip-int-name
no multicast-redirection
```

**Context**
```
config>router>policy-options>policy-statement>default-action
```

**Description**
This command enables a redirection under a filtering policy. The filtering policy in this case becomes a redirection policy and it is defined under the `router>policy-option` hierarchy.

Once the redirection policy is applied to the subscriber, all IGMP messages will be processed per subscriber host before they get redirected to the referenced interface (and possibly service). However, multicast traffic will not be replicated directly per subscriber host but instead it will be forwarded on the interface that is referenced in the redirection policy. The redirected interface must have IGMP enabled.

Currently all traffic is redirected and there is no ability to selectively redirect multicast traffic based on match conditions (multicast-groups, source IP address of IGMP messages, etc). Multicast redirection is supported between VPRN services and also between interfaces within the Global Routing Context. Multicast redirection is not supported between the VPRN services and the Global Routing Context. Multicast redirection is supported in the wholesale/retail VPRN context.

**Default**
disabled

**Parameters**
- `fwd-service service-id` — Specifies the service to which traffic should be redirected. This option is applied only in the VPRN context.
- `ip-int-name` — specifies the alternate interface to which IGMP messages are redirected.

next-hop

**Syntax**
```
next-hop ip-address
no next-hop
```

**Context**
```
config>router>policy-options>policy-statement>default-action
config>router>policy-options>policy-statement>entry>action
```

**Description**
This command assigns the specified next hop IP address to routes matching the policy statement entry. If a next-hop IP address is not specified, the next-hop attribute is not changed.

The `no` form of the command disables assigning a next hop address in the route policy entry.

**Default**
no next-hop — The next hop attribute is not changed.

**Parameters**
- `ip-address` — The next hop IP address in dotted decimal notation.

**Values**
- ipv4-prefix: a.b.c.d (host bits must be 0)
- ipv4-prefix-length: 0 — 32
next-hop-self

Syntax  
[no] next-hop-self

Context  
config>router>policy-options>policy-statement name>default-action  
config>router>policy-options>policy-statement>entry>action

Description  
This command advertises a next hop IP address belonging to this router even if a third-party next hop is  
available to routes matching the policy statement entry.

The no form of the command disables advertising the next-hop-self option for the route policy entry.

Default  
no next-hop-self — The next hop IP address is not changed.

next-hop-self

Syntax  
[no] next-hop-self [multihoming primary-anycast secondary-anycast]

Context  
config>router>policy-option>policy-statement>entry>action

Description  
This command configures the group or neighbor to always set the NEXTHOP path attribute to its own  
physical interface when advertising to a peer. This is primarily used to avoid third-party route advertisements  
when connected to a multi-access network.

In addition, this command can be used to enable and configure the multi-homing reliency mechanism  
replacing the usual BGP nexthop with a configured anycast address.

The no form of the command returns the setting of the BGP next-hop attribute to the default value  
determined by the BGP protocol.

Default  
no next-hop-self

Parameters  
primary-anycast — Specifies the anycast address that the local node will use to replace the BGP nexthop  
address in route updates associated peers.

secondary-address — Specifies the anycast address that the local node is to track.

origin

Syntax  
origin {igp | egp | incomplete}

no origin

Context  
config>router>policy-options>policy-statement name>default-action  
config>router>policy-options>policy-statement>entry>action

Description  
This command sets the BGP origin assigned to routes exported into BGP.

If the routes are exported into protocols other than BGP, this option is ignored.

The no form of the command disables setting the BGP origin for the route policy entry.

Default  
no origin
Parameters

- **igp** — Sets the path information as originating within the local AS.
- **egp** — Sets the path information as originating in another AS.
- **incomplete** — Sets the path information as learned by some other means.

**preference**

**Syntax**

```
preference preference
no preference
```

**Context**

```
config>router>policy-options>policy-statement name=default-action
config>router>policy-options>policy-statement>entry>action>action
```

**Description**

This command assigns a route preference to routes matching the route policy statement entry.

If no preference is specified, the default Route Table Manager (RTM) preference for the protocol is used.

The `no` form of the command disables setting an RTM preference in the route policy entry.

**Default**

`no preference` — No route preference is assigned by the policy entry. The protocol default preference is used.

**Parameters**

- **preference** — The route preference expressed as a decimal integer.

  **Values**

  1 — 255 (0 represents unset - MIB only)

**tag**

**Syntax**

```
tag tag
no tag
```

**Context**

```
config>router>policy-options>policy-statement>default-action
config>router>policy-options>policy-statement>entry>action
```

**Description**

This command assigns an OSPF tag to routes matching the entry. The tag value is used to apply a tag to a route for either an OSPF or RIP route. A hexadecimal value of 4 octets can be entered.

For OSPF, all four octets can be used.

For RIP, only the two most significant octets are used if more than two octets are configured.

The `no` form of the command removes the tag.

**Default**

`no tag`

**Parameters**

- **tag** — Assigns an OSPF, RIP or ISIS tag to routes matching the entry.

  **Values**

  Accepts decimal or hex formats:

  - OSPF and ISIS: `[0x0..0xFFFFFFFF]H`
  - RIP: `[0x0..0xFFFF]H`
type

Syntax  

\begin{verbatim}
  type \{type\}
  no type
\end{verbatim}

Context  

\begin{verbatim}
  config>router>policy-options>policy-statement name>default-action
  config>router>policy-options>policy-statement>entry>action
\end{verbatim}

Description  

This command assigns an OSPF type metric to routes matching the route policy statement entry and being exported into OSPF. The no form of the command disables assigning an OSPF type in the route policy entry.

Default  

\texttt{no type}

Parameters  

\texttt{type} — Specifies the OSPF type metric.

Values  

\begin{itemize}
  \item 1 — Set as OSPF routes with type 1 LSAs
  \item 2 — Set as OSPF routes with type 2 LSAs.
\end{itemize}
Show Commands

policy

Syntax          policy [name | prefix-list name | admin]
Context         show>router
Description     This command displays configured policy statement information.
Parameters      policy name — Displays information similar to the info command for a specific policy-statement. If a name is provided, the matching policy-statement displays.
                  If no statement name is specified, a list of all policies statements and descriptions display.
prefix-list name — Displays the prefix lists configured in the route policy.
admin — If the keyword admin is included, the entire policy option configuration displays, including any un-committed configuration changes. This command is similar to the info command.

Output          Route Policy Output — The following table describes route policy output fields.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>Displays a list of route policy names.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays the description of each route policy.</td>
</tr>
<tr>
<td>Policies</td>
<td>The total number of policies configured.</td>
</tr>
</tbody>
</table>

The following route policy commands are displayed with different command parameter options:

- show router policy on page 777
- show router policy admin on page 778
- show router policy “BGP To RIP” on page 779
- show router policy damping on page 779

Sample Output

The show router policy command displays all configured route policies.

A:ALA-1# show router policy
-----------------------------------------------------------------------------------------------
Route Policies
-----------------------------------------------------------------------------------------------
Policy  Description
-----------------------------------------------------------------------------------------------
Direct And Aggregate  Policy Statement ABC
-----------------------------------------------------------------------------------------------
Policies :
-----------------------------------------------------------------------------------------------
The `show router policy admin` command is similar to the `info` command which displays information about the route policies and parameters.

```
A:ALA-1# show router policy admin
prefix-list "All-Routes"
   prefix 0.0.0.0/0 longer
   prefix 2.0.0.0/8 longer
   prefix 3.0.0.0/8 longer
   prefix 4.0.0.0/8 longer
   prefix 5.0.0.0/8 longer
   prefix 6.0.0.0/8 exact
   prefix 224.0.0.0/24 longer
exit
...
A:ALA-1#
```
The `show router policy name` command displays information about a specific route policy.

```
show router policy "BGP To RIP"

description "Policy Statement For 'BGP To RIP"
    entry 10
        description "Entry For Policy 'BGP To RIP"
            from
                protocol bgp
            exit
to
            protocol rip
            exit
        action accept
            metric set 1
            next-hop 10.0.18.200
tag 0x8008135
        exit
    exit
    default-action reject
```

A:ALA-1#

The `show router policy damping` command displays information about the route policy damping configurations.

```
A:ALA-1# show router policy damping

Route Damping Profiles

    damping "TEST-LOW"
        half-life 22
        max-suppress 720
        reuse 10000
        suppress 15000
    exit
    damping "TEST-HIGH"
        half-life 22
        max-suppress 720
        reuse 1000
        suppress 5000
    exit
    damping "TEST-MEDIUM"
        half-life 22
        max-suppress 720
        reuse 5000
        suppress 11000
    exit

```

A:ALA-1#
Show Commands
Standards and Protocol Support

Standards Compliance
IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1s Multiple Spanning Tree
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ah Provider Backbone Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.1ak Multiple MAC Registration Protocol
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ae 10Gbps Ethernet
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3x Flow Control
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
ITU-T G.8031 Ethernet linear protection switching
ITU-T G.8032 Ethernet Ring Protection Switching (version 2)

Protocol Support

OSPF
RFC 1765 OSPF Database Overflow
RFC 2328 OSPF Version 2
RFC 2370Opaque LSA Support
RFC 2740 OSPF for IPv6 (OSPFv3)
draft-ietf-ospf-ospf-v3-update-14.txt
RFC 3101 OSPF NSSA Option
RFC 3137 OSPF Stub Router Advertisement
RFC 3623 Graceful OSPF Restart – GR helper
RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 4203 - Shared Risk Link Group (SRLG) sub-TLV
RFC 5185 OSPF Multi-Area Adjacency
RFC 3623 Graceful OSPF Restart — GR helper
RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2
RFC 4203 for Shared Risk Link Group (SRLG) sub-TLV

BGP
RFC 1397 BGP Default Route Advertisement
RFC 1772 Application of BGP in the Internet
RFC 1965 Confederations for BGP
RFC 1997 BGP Communities Attribute
RFC 2385 Protection of BGP Sessions via MD5
RFC 2439 BGP Route Flap dampening
RFC 2547bis BGP/MPLS VPNs
RFC 2918 Route Refresh Capability for BGP
RFC 3107 Carrying Label Information in BGP-4
RFC 3392 Capabilities Advertisement with BGP4
RFC 4271 BGP-4 (previously RFC 1771)
RFC 4360 BGP Extended Communities Attribute
RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2547bis BGP/MPLS VPNs)
RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 & 2796)
RFC 4486 Subcodes for BGP Cease Notification Message
RFC 4577 OSPF as the Provider/ Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)
RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 4684 Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)
RFC 4724 Graceful Restart Mechanism for BGP – GR helper
RFC 4760 Multi-protocol Extensions for BGP
RFC 4798 Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
RFC 4893 BGP Support for Four-octet AS Number Space
RFC 5004 Avoid BGP Best Path Transitions from One External to Another
RFC 5065 Confederations for BGP (obsoletes 3065)
RFC 5291 Outbound Route Filtering Capability for BGP-4
RFC 5575 Dissemination of Flow Specification Rules
RFC 5668 4-Octet AS Specific BGP Extended Community
draft-ietf-idr-add-paths
draft-ietf-idr-best-external

IS-IS
RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments
RFC 2763 Dynamic Hostname Exchange for IS-IS
RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
RFC 2973 IS-IS Mesh Groups
RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
RFC 3567 Intermediate System to Intermediate System (ISIS)
RFC 3719 Recommendations for Interoperable Networks using IS-IS
RFC 3784 Intermediate System to Intermediate System (IS-IS)
Extensions for Traffic Engineering (TE)
RFC 3787 Recommendations for Interoperable IP Networks
RFC 3847 Restart Signaling for IS-IS – GR helper
RFC 4205 for Shared Risk Link Group (SRLG) TLV

IPSec
RFC 2401 Security Architecture for the Internet Protocol
RFC 2409 The Internet Key Exchange (IKE)
RFC 3706 IKE Dead Peer Detection
RFC 3947 Negotiation of NAT-Traversal in the IKE
RFC 3948 UDP Encapsulation of IPsec ESP Packets
draft-ietf-ipsec-isakmp-xauth-06.txt – Extended Authentication within ISAKMP/Oakley (XAUTH)
draft-ietf-ipsec-isakmp-modecfg-05.txt – The ISAKMP Configuration Method

IPv6
RFC 1981 Path MTU Discovery for IPv6
RFC 2375 IPv6 Multicast Address Assignments
RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2462 IPv6 Stateless Address Autoconfiguration
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 2529 Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
RFC 2545 Use of BGP-4 Multiprotocol Extension for IPv6 Inter-Domain Routing
RFC 2710 Multicast Listener Discovery (MLD) for IPv6
RFC 3006 Unicast-Prefix-based IPv6 Multicast Addresses
RFC 315 Dynamic Host Configuration Protocol for IPv6
RFC 3587 IPv6 Global Unicast Address Format
RFC3590 Source Address Selection for the Multicast Listener Discovery (MLD) Protocol
RFC 3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6
RFC 4007 IPv6 Scoped Address Architecture
RFC 4193 Unique Local IPv6 Unicast Addresses
RFC 4291 IPv6 Addressing Architecture
RFC 4552 Authentication/Confidentiality for OSPFv3
RFC 4659 BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN
RFC 5072 IP Version 6 over PPP
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
draft-ietf-isis-igm-p2p-over-lan-05.txt
draft-ietf-isis-igp-p2p-over-lan-05.txt

draft-ietf-isis-wg-multi-topology-xx.txt

Multicast
RFC 1112 Host Extensions for IP Multicasting (Snoping)
RFC 2236 Internet Group Management Protocol, (Snoping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snoping)
RFC 2362 Protocol Independent Multicast-Sparse Mode (PIMSM)
RFC 3618 Multicast Source Discovery Protocol (MSDP)
RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
RFC 4604 Using IGMPv3 and MLDv2 for Source-Specific Multicast
RFC 4607 Source-Specific Multicast for IP
RFC 4608 Source-Specific Protocol Independent Multicast in 232/8
RFC 4610 Anycast-RP Using Protocol Independent Multicast (PIM)
RFC 5186, Internet Group Management Protocol Version 3 (IGMPv3)/ Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction
draft-ietf-pim-sm-bsr-06.txt
draft-rosen-vpn-mcast-15.txt Multicast in MPLS/BGP IP VPNs
draft-ietf-mboned-mcast-07.txt Multicast in MPLS/BGP IP VPNs
draft-ietf-mdsdp-mdmib-01.txt
draft-ietf-mdsdp-mdmib-07.txt
RFC 3956: Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address

MPLS — General
RFC 2430 A Provider Architecture DiffServ & TE
RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
RFC 3031 MPLS Architecture
RFC 3032 MPLS Label Stack Encoding
RFC 3443 Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks
RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL
RFC 3140 Per-Hop Behavior Identification Codes
RFC 4905, Encapsulation methods for transport of layer 2 frames over MPLS
RFC 5332 MPLS Multicast Encapsulations

MPLS — LDP
RFC 3037 LDP Applicability
RFC 3478 Graceful Restart Mechanism for LDP – GR helper
RFC 5036 LDP Specification
RFC 5283 LDP extension for Inter-Area LSP
RFC 5443 LDP IGP Synchronization
draft-ietf-mpls-ldp-p2mp-05 LDP Extensions for Point-to-Multipoint and Multipoint-to-Multipoint LSP

MPLS — OAM
RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures
RFC 6425 Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping

RIP
RFC 1058 RIP Version 1
RFC 2082 RIP-2 MD5 Authentication
RFC 2453 RIP Version 2

TCP/IP
RFC 768 UDP
RFC 1350 The TFTP Protocol (Rev. RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 951 BootP (rev)
RFC 1519 CIDR
RFC 1542 Clarifications and Extensions for the Bootstrap Protocol
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Interval and Transfer Size option
RFC 2401 Security Architecture for Internet Protocol
RFC 2428 FTP Extensions for IPv6 and NATs
RFC 3596 DNS Extensions to Support IP version 6
draft-ietf-bfd-mib-00.txt Bidirectional Forwarding Detection Management Information Base
RFC 5880 Bidirectional Forwarding Detection

RFC 5881 BFD IPv4 and IPv6 (Single Hop)
RFC 5883 BFD for Multihop Paths

VRRP
RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol
RFC 3768 Virtual Router Redundancy Protocol
RFC 5798, Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6

PPP
RFC 1332 PPP IPCP
RFC 1377 PPP OSINLCP
RFC 1638/2878PPP BCP
RFC 1661 PPP (rev RFC2151)
RFC 1662 PPP in HDLC-like Framing
RFC 1877 PPP Internet Protocol Control Protocol Extensions for Name Server Addresses
RFC 1989 PPP Link Quality Monitoring
RFC 1990 The PPP Multilink Protocol (MP)
RFC 1994 PPP Challenge Handshake Authentication Protocol (CHAP)
RFC 2615 PPP over SONET/SDH
RFC 2516 A Method for Transmitting PPP Over Ethernet
RFC 2568 The Multi-Class Extension to Multi-Link PPP

Frame Relay
FRF.1.2 - PVC User-to-Network Interface (UNI) Implementation Agreement
FRF.5 - Frame Relay/ATM PVC Network Interworking Implementation
FRF.2.2 - PVC Network-to-Network Interface (NNI) Implementation Agreement.
FRF.12 Frame Relay Fragmentation Implementation Agreement
FRF.16.1 Multilink Frame Relay UNI/NNI Implementation Agreement
ITU-T Q.933 Annex A - Additional procedures for Permanent Virtual Connection (PVC) status management
Standards and Protocols

ATM
- RFC 1626 Default IP MTU for use over ATM AAL5
- RFC 2514 Definitions of Textual Conventions and OBJECT IDENTITIES for ATM Management
- RFC 2515 Definition of Managed Objects for ATM Management
- RFC 2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5
- AF-TM-0121.000 Traffic Management Specification Version 4.1
- ITU-T Recommendation I.610 - B-ISDN Operation and Maintenance Principles and Functions version 11/95
- ITU-T Recommendation I.432.1 – BISDN user-network interface – Physical layer specification: General characteristics
- GR-1248-CORE - Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3
- GR-1113-CORE - Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1
- AF-ILMI-0065.000 Integrated Local Management Interface (ILMI) Version 4.0
- AF-TM-0150.00 Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR
- AF-PHY-0086.001, Inverse Multiplexing for ATM (IMA) Specification Version 1.1

DHCP
- RFC 2131 Dynamic Host Configuration Protocol (REV)
- RFC 3046 DHCP Relay Agent Information Option (Option 82)
- RFC 1534 Interoperation between DHCP and BOOTP

VPLS
- RFC 4762 Virtual Private LAN Services Using LDP
- RFC5501: Requirements for Multicast Support in Virtual Private LAN

Services (previously draft-ietf-l2vpn-vpls-mcast-reqs-04)
draft-ietf-l2vpn-vpls-mcast-reqs-04
draft-ietf-l2vpn-signaling-08

PSEUDOWIRE
- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)
- RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
- RFC 4717 Encapsulation Methods for Transport ATM over MPLS Networks (draft-ietf-pwe3-atm-encap-10.txt)
- RFC 4816 PWE3 ATM Transparent Cell Transport Service (draft-ietf-pwe3-cell-transport-04.txt)
- RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)
- RFC 4694 Encapsulation Methods for Transport of Frame Relay over MPLS Networks (draft-ietf-pwe3-frame-relay-07.txt)
- RFC 4446 IANA Allocations for PWE3
- RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)
- RFC 5085, Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
- RFC 5659 An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge
- draft-ietf-l2vpn-vpls-mcast-reqs-04
- OAM Procedures for VPWS Interworking
- RFC6310, Pseudowire (PW) OAM Message Mapping
draft-ietf-l2vpn-arp-mediation-19.txt,
ARPMediation for IP Interworking of Layer 2 VPN
RFC6073, Segmented Pseudowire (draft-ietf-pwe3-segmented-pw-18.txt)
draft-ietf-pwe3-segmented-pw-18.txt
draft-ietf-pwe3-dynamic-m-s-pw-14.txt,
Dynamic Placement of Multi Segment Pseudo Wires
draft-ietf-pwe3-redundancy-bit-06.txt,
Pseudowire Preferential Forwarding Status bit definition
draft-ietf-pwe3-redundancy-06.txt,
Pseudowire (PW) Redundancy
RFC6391 Flow Aware Transport of Pseudowires over an MPLS PSN
MFA Forum 9.0.0 The Use of Virtual trunks for ATM/MPLS Control Plane Interworking
MFA Forum 12.0.0 Multiservice Interworking - Ethernet over MPLS
MFA forum 13.0.0 - Fault Management for Multiservice Interworking v1.0
MFA Forum 16.0.0 – Multiservice Interworking - IP over MPLS

ANCP/L2CP
- RFC5851 ANCP framework
draft-ietf-ancp-protocol-02.txt ANCP Protocol

Voice/Video Performance
- ITU-T Rec. P.564 - Conformance testing for voice over IP transmission quality assessment models
- ITU-T G.1020 - Appendix I - Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks- Mean Absolute Packet Delay Variation & Markov Models.

CIRCUIT EMULATION
- RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
MEF-8 Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks, October 2004

RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks

SONET/SDH
ITU-G.841 Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

RADIUS
RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH
RFC 4250 The Secure Shell (SSH) Protocol
draft-ietf-seesh-architecture.txt SSH Protocol Architecture
draft-ietf-seesh-userauth.txt SSH Authentication Protocol
draft-ietf-seesh-transport.txt SSH Transport Layer Protocol
draft-ietf-seesh-connection.txt SSH Connection Protocol
draft-ietf-seesh-newmodes.txt SSH Transport Layer Encryption Modes

TACACS+
draft-grant-tacacs-02.txt

Timing
ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008
ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.


NETWORK MANAGEMENT
ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1657 BGP4-MIB
RFC 1724 RIPv2-MIB
RFC 1850 OSPF-MIB
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2138 RADIUS
RFC 2206 RSVP-MIB
RFC 2452 IPv6 Management Information Base for the Transmission Control Protocol
RFC 2454 IPv6 Management Information Base for the User Datagram Protocol
RFC 2465 Management Information Base for IPv6: Textual Conventions and General Group
RFC 2558 SONET-MIB
RFC 2571 SNMP-Framework MIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-Target-&-notification-MIB
RFC 2574 SNMP-User-based-SMMIB
RFC 2575 SNMP-View-based-ACM-MIB
RFC 2576 SNMP-Community-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 Inverted-stack-MIB
RFC 2987 VRRP-MIB
RFC 3014 Notification-log MIB
RFC 3019 IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 Simple Network Management Protocol (SNMP) Applications
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 SNMP MIB
RFC 4292 IP-Forward-MIB
RFC 4293 MIB for the Internet Protocol
draft-ietf-ospf-mib-update-04.txt
draft-ietf-mpls-lsr-mib-06.txt
draft-ietf-mpls-te-mib-04.txt
draft-ietf-isis-wg-mib-05.txt
IANA-Iftype-MIB
IEEE8023-LAG-MIB

Proprietary MIBs
TIMETRA-APS-MIB.mib
TIMETRA-ATM-MIB.mib
TIMETRA-BGP-MIB.mib
TIMETRA-BSX-NG-MIB.mib
TIMETRA-CAPABILITY-7750-V4v0.mib
Standards and Protocols

TIMETRA-CFLOWD-MIB.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IGMP-MIB.mib
TIMETRA-ISIS-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-NG-BGP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-OSPF-NG-MIB.mib
TIMETRA-OSPF-V3-MIB.mib
TIMETRA-PIM-NG-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-RIP-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SUBSCRIBER-MGMTMIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRRP-MIB.mib
TIMETRA-VRTR-MIB.mib
INDEX

B

BGP
  overview 542
  confederations 553
  group configuration and peers 544
  hierarchical levels 545
  interactions and dependencies 567
  message types 542
  route damping 570
  route reflection 545
  configuring 584
    autonomous system 587
    basic 584
    BGP parameters
      group 593
      neighbor 594
    command reference 603
    confederation 596
    overview 582
    route reflection 591, 595
    router ID 588
    management tasks 597

I

IP Router
  configuring
    basic 61
    service management tasks 81

IS-IS
  overview 432
    ISO network addressing 436
    PDU configuration 439
    routing 433
    terminology 435
  configuring
    area address attributes 446
    basic 449
    command reference 471
    enabling IS-IS 452
    global parameters 455
    interface level capabilities 447
    interface parameters 456
    ISO area addresses 454
    level parameters 452
    management tasks 461
    overview 446
    router levels 446

M

Multicast 21
  IGMP 27
  PIM 30

O

OSPF
  overview 286
    AS areas 287
      backbone 287
    NSSA 289
    stub 288
    authentication 299
    IP subnets 300
    LSAs 298
    metrics 298
    neighbors and adjacencies 297
    virtual links 296
  configuring 315
    area interface 323
    authentication 325
    basic 315
    command reference 339
    designated router 328
    management tasks 334
    NSSA 320
    OSPF area 318
    overview 314
    route preferences 332
    route summaries 330
    router ID 316
    stub area 319
    virtual link 321
R

RIP
  overview  232
  authentication  233
  hierarchy  237
  import/export policies  234
  metrics  234
  packet format  235
  ripv1  236
  ripv2  236
  timers  234
  version types  233
configuring
  basic  243
  command reference  255
  interfaces  245
  management tasks  253
  overview  242
  RIP parameters  248
    global  250
    group  251
    neighbor  252
  route policy  246

Route policies
  overview  704
  damping  727
  default actions  723
  policy evaluation  724
  policy statements  705
  regular expressions  709
  when to use  718
configuring
  beginning  731
  command reference  745
  community list  735
  creating a route policy  732
  damping  736
  default action  733
  entry  734
  management tasks  741
  overview  722
  prefix list  737