THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATIONS, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2016 Cisco Systems, Inc. All rights reserved.
CONTENTS

Preface xi

Changes to This Document xi

Obtaining Documentation and Submitting a Service Request xi

CHAPTER 1 Implementing Layer-2 Multicast with IGMP Snooping 1

Prerequisites for IGMP Snooping 2

Restrictions for IGMP Snooping 2

Information About IGMP Snooping 2

IGMP Snooping Overview 2

Description of Basic Functions 2

High Availability Features 3

Bridge Domain Support 3

Multicast Router and Host Ports 3

Multicast Router Discovery and Static Configuration 4

Multicast Traffic Handling within a Bridge Domain with IGMP Snooping Enabled 4

Multichassis Link Aggregation 5

Information About IGMP Snooping Configuration Profiles 6

Creating Profiles 6

Attaching and Detaching Profiles 6

Changing Profiles 7

Configuring Access Control 7

Default IGMP Snooping Configuration Settings 9

IGMP Snooping Configuration at the Bridge Domain Level 10

IGMP Minimum Version 10

System IP Address 10

Group Membership Interval, Robustness Variable, and Query Interval 10

Report Suppression (IGMPv2) and Proxy Reporting (IGMPv3) 11
Contents

Group Leave Processing 11
Reaction to Topology Change Notifications 13
IGMP Snooping Packet Checks 14
Startup Query Configuration 14
IGMP Snooping Configuration at the Host Port Level 15
Router Guard and Static Mrouter 15
Immediate-Leave 15
Static Groups 15

Internal Querier 16
When to Use an Internal Querier 16
Internal Querier Default Configuration 16
Internal Querier Processing 17
Querier Election for One Active Querier 17
Internal Querier Reaction to TCNs 18

How to Configure IGMP Snooping 18
Creating an IGMP Snooping Profile 18
Where to Go Next 19
Attaching a Profile and Activating IGMP Snooping on a Bridge Domain 19
Detaching a Profile and Deactivating IGMP Snooping on a Bridge Domain 21
Attaching and Detaching Profiles to Ports Under a Bridge 22
Adding Static Mrouter Configuration to a Profile 24
Where to Go Next 25
Adding Router Guard to a Profile 25
Where to Go Next 26
Configuring Immediate-Leave 27
Where to Go Next 28
Configuring Static Groups 28
Where to Go Next 29
Configuring an Internal Querier 29
Where to Go Next 30
Verifying Multicast Forwarding 30
Configuring Group Limits 31
Configuring route-policy 31
Configuring group limit 32
Configuring access-groups 33
Configuration Examples for IGMP Snooping 34
   Configuring IGMP Snooping on Physical Interfaces Under a Bridge: Example 34
   Configuring IGMP Snooping on VLAN Interfaces Under a Bridge: Example 35
   Configuring IGMP Snooping on Ethernet Bundles Under a Bridge: Example 35
   Configuring IGMP Snooping on VFIs Under a Bridge: Example 37
   Configuring IGMP access-groups 39
   Configuring IGMP Snooping over MCLAG: Example 40
      Case 1: Downstream MCLAG 40
      Case 2: Upstream MCLAG 45
Additional References 50

CHAPTER 2 Implementing Layer-3 Multicast Routing on Cisco IOS XR Software 53
   Prerequisites for Implementing Multicast Routing 55
   Information About Implementing Multicast Routing 55
      Key Protocols and Features Supported in the Cisco IOS XR Software Multicast Routing Implementation 55
      Multicast Routing Functional Overview 56
      Multicast Routing Implementation 57
   PIM-SM, PIM-SSM, and PIM-BIDIR 58
      PIM-SM Operations 58
      PIM-SSM Operations 58
      PIM-Bidirectional Operations 58
      Restrictions for PIM-SM and PIM-SSM, and PIM BIDIR 59
   Internet Group Management Protocol 59
      IGMP Versions 59
      IGMP Routing Example 60
   Protocol Independent Multicast 60
      PIM-Sparse Mode 61
      PIM-Source Specific Multicast 61
      PIM-Bidirectional Mode 62
   PIM Shared Tree and Source Tree (Shortest Path Tree) 63
   Multicast-Intact 64
   Designated Routers 65
   Rendezvous Points 66
   Auto-RP 67
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM Bootstrap Router</td>
<td>68</td>
</tr>
<tr>
<td>Reverse-Path Forwarding</td>
<td>68</td>
</tr>
<tr>
<td>Multicast VPN</td>
<td>68</td>
</tr>
<tr>
<td>Multicast VPN Routing and Forwarding</td>
<td>69</td>
</tr>
<tr>
<td>Multicast Distribution Tree Tunnels</td>
<td>70</td>
</tr>
<tr>
<td>InterAS Support on Multicast VPN</td>
<td>70</td>
</tr>
<tr>
<td>IPv6 Connectivity over MVPN</td>
<td>73</td>
</tr>
<tr>
<td>BGP Requirements</td>
<td>73</td>
</tr>
<tr>
<td>MVPN Static P2MP TE</td>
<td>73</td>
</tr>
<tr>
<td>Multitopology Routing</td>
<td>74</td>
</tr>
<tr>
<td>Multicast VPN Extranet Routing</td>
<td>75</td>
</tr>
<tr>
<td>Information About Extratets</td>
<td>75</td>
</tr>
<tr>
<td>Information About the Extranet MVPN Routing Topology</td>
<td>76</td>
</tr>
<tr>
<td>RPF Policies in an Extranet</td>
<td>78</td>
</tr>
<tr>
<td>Multicast VPN Hub and Spoke Topology</td>
<td>78</td>
</tr>
<tr>
<td>Realizing the Hub and Spoke Topology</td>
<td>79</td>
</tr>
<tr>
<td>Label Switched Multicast (LSM) Multicast Label Distribution Protocol (mLDP) based</td>
<td></td>
</tr>
<tr>
<td>Multicast VPN (mVPN) Support</td>
<td>80</td>
</tr>
<tr>
<td>Benefits of LSM MLDP based MVPN</td>
<td>80</td>
</tr>
<tr>
<td>Configuring MLDP MVPN</td>
<td>80</td>
</tr>
<tr>
<td>P2MP and MP2MP Label Switched Paths</td>
<td>81</td>
</tr>
<tr>
<td>Packet Flow in mLDP-based Multicast VPN</td>
<td>82</td>
</tr>
<tr>
<td>Realizing a mLDP-based Multicast VPN</td>
<td>82</td>
</tr>
<tr>
<td>Characteristics of mLDP Profiles</td>
<td>82</td>
</tr>
<tr>
<td>Configuration rules for profiles</td>
<td>88</td>
</tr>
<tr>
<td>MLDP inband signaling</td>
<td>89</td>
</tr>
<tr>
<td>Summary of Supported MVPN Profiles</td>
<td>89</td>
</tr>
<tr>
<td>Configuration Process for MLDP MVPN (Intranet)</td>
<td>90</td>
</tr>
<tr>
<td>MVPN over GRE</td>
<td>92</td>
</tr>
<tr>
<td>Native Multicast</td>
<td>93</td>
</tr>
<tr>
<td>GRE Limitations</td>
<td>94</td>
</tr>
<tr>
<td>Signaling and RPF on GRE Tunnels</td>
<td>95</td>
</tr>
<tr>
<td>PIM Registration</td>
<td>95</td>
</tr>
<tr>
<td>Auto-RP</td>
<td>95</td>
</tr>
<tr>
<td>Multicast Source Discovery Protocol</td>
<td>96</td>
</tr>
</tbody>
</table>
VRF-aware MSDP 96
Multicast Nonstop Forwarding 96
Multicast Configuration Submodes 97
  Multicast-Routing Configuration Submode 97
  PIM Configuration Submode 97
  IGMP Configuration Submode 98
  MLD Configuration Submode 98
  MSDP Configuration Submode 98
Understanding Interface Configuration Inheritance 98
Understanding Interface Configuration Inheritance Disablement 99
Understanding Enabling and Disabling Interfaces 99
Multicast Routing Information Base 100
Multicast Forwarding Information Base 100
MSDP MD5 Password Authentication 100
Overriding VRFs in IGMP Interfaces 101
VRF support for MLD 101
Support for Satellite nV 101
How to Implement Multicast Routing 102
  Configuring PIM-SM and PIM-SSM 102
  Configuring PIM-SSM for Use in a Legacy Multicast Deployment 104
    Restrictions for PIM-SSM Mapping 104
    Configuring a Set of Access Control Lists for Static SSM Mapping 104
    Configuring a Set of Sources for SSM Mapping 105
Configuring a Static RP and Allowing Backward Compatibility 106
Configuring Auto-RP to Automate Group-to-RP Mappings 108
Configuring the Bootstrap Router 109
Calculating Rates per Route 112
Configuring Multicast Nonstop Forwarding 114
Configuring Multicast VPN 116
  Prerequisites for Multicast VPN 117
  Restrictions for Multicast VPN for Multicast Routing 117
  Enabling a VPN for Multicast Routing 118
  Specifying the PIM VRF Instance 120
  Specifying the IGMP VRF Instance 121
  Configuring the MDT Source per VRF 122
Configuring Label Switched Multicast 124
Verification of LSM mLDP based MVPN Configuration 129
Configuring MVPN Static P2MP-TE 132
Configuring MVPN P2MP on Ingress PE 132
Configuring MVPN P2MP BGP 134
Configuring MVPN P2MP on Egress PE 138
Configuring MVPN InterAS Options 140
Configuring a PE Router for MVPN InterAS Option B or C 140
Configuring ASBR Router for MVPN InterAS Option B or C 148
Configuring RR for MVPN InterAS Option C 154
Configuring Multitopology Routing 159
Restrictions for Configuring Multitopology Routing 160
Information About Multitopology Routing 160
Configuring an RPF Topology in PIM 161
Configuring MVPN Extranet Routing 162
Prerequisites for MVPN Extranet Routing 162
Restrictions for MVPN Extranet Routing 163
Configuring VPN Route Targets 163
Interconnecting PIM-SM Domains with MSDP 165
Controlling Source Information on MSDP Peer Routers 167
Configuring MSDP MD5 Password Authentication 170
Configuring VRF for MSDP 171
Multicast only fast reroute (MoFRR) 171
Operating Modes of MoFRR 172
Restrictions 172
Configuring MoFRR 172
RIB-based MoFRR 172
Flow-based MoFRR 173
Configuring Route Policy for Static RPF 175
Point-to-Multipoint Traffic Engineering Label-Switched Multicast 176
Point to Multipoint LSP(P2MP) 176
Multicast Routing Protocol support for P2MP 177
Enabling Multicast Forwarding Over Tunnel Interface (at Ingress Node) 177
P2MP configurations at egress node and bud node 178
Configuring Static Reverse Path Forwarding (RPF) 178
Additional References 237
Preface

From Release 6.1.1 onwards, Cisco introduces support for the 64-bit Linux-based IOS XR operating system. Extensive feature parity is maintained between the 32-bit and 64-bit environments. Unless explicitly marked otherwise, the contents of this document are applicable for both the environments. For more details on Cisco IOS XR 64 bit, refer to the Release Notes for Cisco ASR 9000 Series Routers, Release 6.1.1 document.

The preface contains these sections:

- Changes to This Document, page xi
- Obtaining Documentation and Submitting a Service Request, page xi

Changes to This Document

This table lists the technical changes made to this document since it was first printed.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>OL-26037-02</td>
<td>June 2012</td>
<td>Republished with documentation updates for Cisco IOS XR Release 4.2.1 features.</td>
</tr>
<tr>
<td>OL-26037-01</td>
<td>December 2011</td>
<td>Initial release of this document.</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.
Implmenting Layer-2 Multicast with IGMP Snooping

Internet Group Management Protocol (IGMP) snooping restricts multicast flows at Layer 2 to only those segments with at least one interested receiver. This module describes how to implement IGMP snooping on Cisco ASR 9000 Series Routers.

**Feature History for IGMP Snooping**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>Release 3.9.2</td>
<td>Support was added for the following features:</td>
</tr>
<tr>
<td></td>
<td>• IGMP snooping group limits and access groups.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>Support was added for the following features:</td>
</tr>
<tr>
<td></td>
<td>• Multicast redundancy using Multi-Chassis Link Aggregation (MC-LAG).</td>
</tr>
</tbody>
</table>

• Prerequisites for IGMP Snooping, page 2
• Restrictions for IGMP Snooping, page 2
• Information About IGMP Snooping, page 2
• How to Configure IGMP Snooping, page 18
• Configuration Examples for IGMP Snooping, page 34
• Additional References, page 50
Prerequisites for IGMP Snooping

The following prerequisites must be satisfied before implementing IGMP snooping:

- The network must be configured with a Layer 2 VPN (L2VPN).
- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Restrictions for IGMP Snooping

- IGMP snooping is supported only under L2VPN bridge domains.
- Explicit host tracking (an IGMPv3 snooping feature) is not supported.
- IPv6 Multicast Listener Discovery (MLD) snooping is not supported.
- IGMPv1 is not supported.

Information About IGMP Snooping

IGMP Snooping Overview

Description of Basic Functions

IGMP snooping provides a way to constrain multicast traffic at Layer 2. By snooping the IGMP membership reports sent by hosts in the bridge domain, the IGMP snooping application can set up Layer 2 multicast forwarding tables to deliver traffic only to ports with at least one interested member, significantly reducing the volume of multicast traffic.

Configured at Layer 3, IGMP provides a means for hosts in an IPv4 multicast network to indicate which multicast traffic they are interested in and for routers to control and limit the flow of multicast traffic in the network at Layer 3.

IGMP snooping uses the information in IGMP membership report messages to build corresponding information in the forwarding tables to restrict IP multicast traffic at Layer 2. The forwarding table entries are in the form <Route, OIF List>, where:

- Route is a <*, G> route or <S, G> route.
- OIF List comprises all bridge ports that have sent IGMP membership reports for the specified route plus all multicast router (mrouter) ports in the bridge domain.

Implemented in a multicast network, IGMP snooping has the following attributes:

- In its basic form, it reduces bandwidth consumption by reducing multicast traffic that would otherwise flood an entire VPLS bridge domain.
With the use of some optional configurations, it provides security between bridge domains by filtering the IGMP reports received from hosts on one bridge port and preventing leakage towards the hosts on other bridge ports.

Using optional configurations, reduces the traffic impact on upstream IP multicast routers by suppressing IGMP membership reports (IGMPv2) or by acting as an IGMP proxy reporter (IGMPv3) to the upstream IP multicast router.

High Availability Features

All high availability features apply to the IGMP snooping processes with no additional configuration beyond enabling IGMP snooping. The following high availability features are supported:

- Process restarts
- RP Failover
- Stateful Switch-Over (SSO)
- Non-Stop Forwarding (NSF)—Forwarding continues unaffected while the control plane is restored following a process restart or route processor (RP) failover.
- Line card online insertion and removal (OIR)

Bridge Domain Support

IGMP snooping operates at the bridge domain level. When IGMP snooping is enabled on a bridge domain, the snooping functionality applies to all ports under the bridge domain, including:

- Physical ports under the bridge domain.
- Ethernet flow points (EFPs)—An EFP can be a VLAN, VLAN range, list of VLANs, or an entire interface port.
- Pseudowires (PWs) in VPLS bridge domains.
- Ethernet bundles—Ethernet bundles include IEEE 802.3ad link bundles and Cisco EtherChannel bundles. From the perspective of the IGMP snooping application, an Ethernet bundle is just another EFP. The forwarding application in the Cisco ASR 9000 Series Routers randomly nominates a single port from the bundle to carry the multicast traffic.

Multicast Router and Host Ports

IGMP snooping classifies each port (for example, EFPs, PWs, physical ports, or EFP bundles) as one of the following:

- Multicast router ports (mrouter ports)—These are ports to which a multicast-enabled router is connected. Mrouter ports are usually dynamically discovered, but may also be statically configured. Multicast traffic is always forwarded to all mrouter ports, except when an mrouter port is the ingress port.
- Host ports—Any port that is not an mrouter port is a host port.
Multicast Router Discovery and Static Configuration

IGMP snooping discovers mrouter ports dynamically. You can also explicitly configure a port as an mrouter
port.

- Discovery—IGMP snooping identifies upstream mrouter ports in the bridge domain by snooping IGMP
  query messages and Protocol Independent Multicast Version 2 (PIMv2) hello messages. Snooping PIMv2
  hello messages identifies IGMP nonqueriers in the bridge domain.

- Static configuration—You can statically configure a port as an mrouter port with the mrouter command
  in a profile attached to the port. Static configuration can help in situations when incompatibilities with
  non-Cisco equipment prevent dynamic discovery.

The router-guard command prevents a port from becoming a dynamically discovered mrouter port by filtering
out multicast router messages, including IGMP queries and PIM messages. You can configure a port with the
router-guard command and then configure it as a static mrouter. See the Router Guard and Static Mrouter,
on page 15 for more information about configuring router-guard and mrouter commands on the same port.

Multicast Traffic Handling within a Bridge Domain with IGMP Snooping Enabled

The following tables describe traffic handling behaviors by IGMP snooping mrouter and host ports. Table 1:
Multicast Traffic Handling for an IGMPv2 Querier, on page 4 describes traffic handling for an IGMPv2
querier. Table 2: Multicast Traffic Handling for an IGMPv3 Querier, on page 5 applies to an IGMPv3
querier.

By default, IGMP snooping supports IGMPv2 and IGMPv3. The version of the IGMP querier discovered in
the bridge domain determines the operational version of the snooping processes. If you change the default,
configuring IGMP snooping to support a minimum version of IGMPv3, IGMP snooping ignores any IGMPv2
queriers.

Table 1: Multicast Traffic Handling for an IGMPv2 Querier

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Received on MRouter Ports</th>
<th>Received on Host Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP multicast source traffic</td>
<td>Forwards to all mrouter ports and to host ports that indicate interest.</td>
<td>Forwards to all mrouter ports and to host ports that indicate interest.</td>
</tr>
<tr>
<td>IGMP general queries</td>
<td>Forwards to all ports.</td>
<td>—</td>
</tr>
<tr>
<td>IGMP group-specific queries</td>
<td>Forwards to all other mrouter ports.</td>
<td>Dropped</td>
</tr>
<tr>
<td>IGMPv2 joins</td>
<td>Examines (snoops) the reports.</td>
<td>Examines (snoops) the reports.</td>
</tr>
<tr>
<td></td>
<td>- If report suppression is enabled, forwards first join for a new group or first join following a general query for an existing group.</td>
<td>- If report suppression is enabled, forwards first join for a new group or first join following a general query for an existing group.</td>
</tr>
<tr>
<td></td>
<td>- If report suppression is disabled, forwards on all mrouter ports.</td>
<td>- If report suppression is disabled, forwards on all mrouter ports.</td>
</tr>
</tbody>
</table>
### Table 2: Multicast Traffic Handling for an IGMPv3 Querier

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>Received on MRouter Ports</th>
<th>Received on Host Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMPv3 reports</td>
<td>Ignores</td>
<td>Ignores</td>
</tr>
<tr>
<td>IGMPv2 leaves</td>
<td>Invokes last member query processing.</td>
<td>Invokes last member query processing.</td>
</tr>
<tr>
<td>IP multicast source traffic</td>
<td>Forwards to all mrouter ports and to host ports that indicate interest.</td>
<td>Forwards to all mrouter ports and to host ports that indicate interest.</td>
</tr>
<tr>
<td>IGMP general queries</td>
<td>Forwards to all ports.</td>
<td>—</td>
</tr>
<tr>
<td>IGMP group-specific queries</td>
<td>If received on the querier port floods on all ports.</td>
<td>—</td>
</tr>
<tr>
<td>IGMPv2 joins</td>
<td>Handles as IGMPv3 IS_EX{} reports.</td>
<td>Handles as IGMPv3 IS_EX{} reports.</td>
</tr>
<tr>
<td>IGMPv3 reports</td>
<td>• If proxy reporting is enabled—For state changes or source-list changes, generates a state change report on all mrouter ports.</td>
<td>• If proxy reporting is enabled—For state changes or source-list changes, generates a state change report on all mrouter ports.</td>
</tr>
<tr>
<td></td>
<td>• If proxy reporting is disabled—Forwards on all mrouter ports.</td>
<td>• If proxy reporting is disabled—Forwards on all mrouter ports.</td>
</tr>
<tr>
<td>IGMPv2 leaves</td>
<td>Handles as IGMPv3 IS_IN{} reports.</td>
<td>Handles as IGMPv3 IS_IN{} reports.</td>
</tr>
</tbody>
</table>

### Multichassis Link Aggregation

The Multichassis Link Aggregation (MC-LAG) feature provides a simple redundancy mechanism for the Digital Subscriber Line Access Multiplexer (DSLAM) to access Cisco ASR 9000 Series Routers. The redundancy is achieved by allowing a dual-homed connection to two or more Cisco ASR 9000 Series Routers.

The DSLAM is known as a Dual-Homed Device (DHD) and the Cisco ASR 9000 Series Router is known as a Point of Attachment (PoA). An MC-LAG is assigned into a Redundancy Group (RG). The Cisco ASR 9000 Series Routers (PoAs) that manage a given MC-LAG are members of this RG. There may be multiple MC-LAGs in the RG. This indicates that the same RG may cover MC-LAG connections to other DSLAMs. Hence, the RG is uniquely identified on the PoAs by an Redundancy Group Identifier (RGID). The MC-LAG is identified...
on each PoA by a unique Redundancy Object Identifier, also termed as ROID. If VLAN sub-interfaces are configured on the MC-LAG, then each VLAN sub-interface has a unique ROID.

IGMP Snooping on the Cisco ASR 9000 Series Router supports MC-LAG configurations looking either downstream towards a DSLAM or upstream towards a multicast router.

---

**Note**

Both the active and standby POAs must have the same configuration for the MC-LAG feature to work.

For more information on configuring link bundling and protocols used, see the Configuring Link Bundling chapter in Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide.

**Information About IGMP Snooping Configuration Profiles**

To enable IGMP snooping on a bridge domain, you must attach a profile to the bridge domain. The minimum configuration is an empty profile. An empty profile enables the default configuration options and settings for IGMP snooping, as listed in the Default IGMP Snooping Configuration Settings, on page 9.

You can attach IGMP snooping profiles to bridge domains or to ports under a bridge domain. The following guidelines explain the relationships between profiles attached to ports and bridge domains:

- Any IGMP profile attached to a bridge domain, even an empty profile, enables IGMP snooping. To disable IGMP snooping, detach the profile from the bridge domain.
- An empty profile configures IGMP snooping on the bridge domain and all ports under the bridge using default configuration settings.
- A bridge domain can have only one IGMP snooping profile attached to it (at the bridge domain level) at any time. Profiles can be attached to ports under the bridge, one profile per port.
- Port profiles are not in effect if the bridge domain does not have a profile attached to it.
- IGMP snooping must be enabled on the bridge domain for any port-specific configurations to be in effect.
- If a profile attached to a bridge domain contains port-specific configuration options, the values apply to all of the ports under the bridge, including all mrouter and host ports, unless another port-specific profile is attached to a port.
- When a profile is attached to a port, IGMP snooping reconfigures that port, disregarding any port configurations that may exist in the bridge-level profile.

**Creating Profiles**

To create a profile, use the `igmp snooping profile` command in global configuration mode.

**Attaching and Detaching Profiles**

To attach a profile to a bridge domain, use the `igmp snooping profile` command in l2vpn bridge group bridge domain configuration mode. To attach a profile to a port, use the `igmp snooping profile` command in the interface configuration mode under the bridge domain. To detach a profile, use the `no` form of the command in the appropriate configuration mode.
When you detach a profile from a bridge domain or a port, the profile still exists and is available for use at a later time. Detaching a profile has the following results:

- If you detach a profile from a bridge domain, IGMP snooping is deactivated in the bridge domain.
- If you detach a profile from a port, IGMP snooping configuration values for the port are instantiated from the bridge domain profile.

Changing Profiles

You cannot make changes to an active profile. An active profile is one that is currently attached.

If you need to change an active profile, you must detach it from all bridges or ports, change it, and reattach it.

Another way to do this is to create a new profile incorporating the desired changes and attach it to the bridges or ports, replacing the existing profile. This deactivates IGMP snooping and then reactivates it with parameters from the new profile.

Configuring Access Control

Access control configuration is the configuration of access groups and weighted group limits.

The role of access groups in IGMP v2/v3 message filtering is to permit or deny host membership requests for multicast groups (*,G) and multicast source groups (S,G). This is required to provide black-and-white list access to IPTV channel packages.

Weighted group limits restrict the number of IGMP v2/v3 groups, in which the maximum number of concurrently allowed multicast channels can be configured on a per EFP- and per PW-basis.

IGMP Snooping Access Groups

Although Layer-3 IGMP routing also uses the `igmp access-group` command in support of access groups, the support is not the same in Layer-2 IGMP, because the Layer-3 IGMP routing access group feature does not support source groups.

Access groups are specified using an extended IP access list referenced in an IGMP snooping profile that you attach to a bridge domain or a port.

Note

A port-level access group overrides any bridge domain-level access group.

The `access-group` command instructs IGMP snooping to apply the specified access list filter to received membership reports. By default, no access list is applied.

Changes made to the access-list referenced in the profile (or a replacement of the access-list referenced in the igmp snooping profile) will immediately result in filtering the incoming igmp group reports and the existing group states accordingly, without the need for a detach-reattach of the igmp snooping profile in the bridge-domain, each time such a change is made.

IGMP Snooping Group Weighting

To limit the number of IGMP v2/v3 groups, in which the maximum number of concurrently allowed multicast channels must be configurable on a per EFP-basis and per PW-basis, configure group weighting.
IGMP snooping limits the membership on a bridge port to a configured maximum, but extends the feature to support IGMPv3 source groups and to allow different weights to be assigned to individual groups or source groups. This enables the IPTV provider, for example, to associate standard and high-definition IPTV streams, as appropriate, to specific subscribers.

This feature does not limit the actual multicast bandwidth that may be transmitted on a port. Rather, it limits the number of IGMP groups and source-groups, of which a port can be a member. It is the responsibility of the IPTV operator to configure subscriber membership requests to the appropriate multicast flows.

The **group policy** command, which is under igmp-snooping-profile configuration mode, instructs IGMP snooping to use the specified route policy to determine the weight contributed by a new <*,G> or <S,G> membership request. The default behavior is for there to be no group weight configured.

The **group limit** command specifies the group limit of the port. No new group or source group is accepted if its contributed weight would cause this limit to be exceeded. If a group limit is configured (without group policy configuration), a <S/*,G> group state will have a default weight of 1 attributed to it.

---

**Note**

By default, each group or source-group contributes a weight of 1 towards the group limit. Different weights can be assigned to groups or source groups using the group policy command.

The group limit policy configuration is based on these conditions:

- Group weight values for <*,G> and <S,G> membership are configured in a Route Policy, that is included in an igmp snooping profile attached to a BD or port.

- Port level weight policy overrides any bridge domain level policy, if group-limit is set and route-policy is configured.

- If there is no policy configured, each group weight is counted equally and is equal to 1.

- If policy has been configured, all matching groups get weight of 1 and un-matched groups have 0 weight.
# Default IGMP Snooping Configuration Settings

**Table 3: IGMP Snooping Default Configuration Values**

<table>
<thead>
<tr>
<th>Scope</th>
<th>Feature</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Domain</td>
<td>IGMP snooping</td>
<td>Disabled on a bridge domain until an enabling IGMP profile is attached to the bridge domain.</td>
</tr>
<tr>
<td></td>
<td>internal querier</td>
<td>None configured</td>
</tr>
<tr>
<td></td>
<td>last-member-query-count</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>last-member-query-interval</td>
<td>1000 (milliseconds)</td>
</tr>
<tr>
<td></td>
<td>minimum-version</td>
<td>2 (supporting IGMPv2 and IGMPv3)</td>
</tr>
<tr>
<td></td>
<td>querier query-interval</td>
<td>60 (seconds)</td>
</tr>
<tr>
<td></td>
<td>report-suppression</td>
<td>Enabled (enables report suppression for IGMPv2 and proxy-reporting for IGMPv3)</td>
</tr>
<tr>
<td></td>
<td>querier robustness-variable</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>router alert check</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>tcn query solicit</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>tcn flood</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>ttl-check</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td>unsolicited-report-timer</td>
<td>1000 (milliseconds)</td>
</tr>
<tr>
<td>Port</td>
<td>immediate-leave</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>mrouter</td>
<td>No static mrouteers configured; dynamic discovery occurs by default.</td>
</tr>
<tr>
<td></td>
<td>router guard</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>static group</td>
<td>None configured</td>
</tr>
</tbody>
</table>
IGMP Snooping Configuration at the Bridge Domain Level

IGMP Minimum Version

The `minimum-version` command determines which IGMP versions are supported by IGMP snooping in the bridge domain:

- When minimum-version is 2, IGMP snooping intercepts IGMPv2 and IGMPv3 messages. This is the default value.
- When minimum-version is 3, IGMP snooping intercepts only IGMPv3 messages and drops all IGMPv2 messages.

IGMPv1 is not supported. The scope for this command is the bridge domain. The command is ignored in a profile attached to a port.

System IP Address

The `system-ip-address` command configures an IP address for IGMP snooping use. If not explicitly configured, the default address is 0.0.0.0. The default is adequate except in the following circumstances:

- If you are configuring an internal querier. The internal querier cannot use 0.0.0.0.
- If the bridge needs to communicate with an IGMP router that does not accept the 0.0.0.0 address.

The IGMP snooping system IP address is used in the following ways:

- The internal-querier sends queries from the system IP address. An address other than the default 0.0.0.0 must be configured.
- IGMPv3 sends proxy reports from the system IP address. The default address 0.0.0.0 is preferred but may not be acceptable to some IGMP routers.
- In response to topology change notifications (TCNs) in the bridge domain, IGMP snooping sends global-leaves from the system IP address. The default address 0.0.0.0 is preferred but may not be acceptable to some IGMP routers.

Group Membership Interval, Robustness Variable, and Query Interval

The group membership interval (GMI) controls when IGMP snooping expires stale group membership states. The `show igmp snooping group` command shows groups with an expiry time of 0 until that stale state is cleaned up following the next query interval.

The GMI is calculated as:

\[ GMI = (\text{robustness-variable} \times \text{query-interval}) + \text{maximum-response-time} \]

where:

- maximum-response-time (MRT) is the amount of time during which receivers are required to report their membership state.
- robustness-variable is an integer used to influence the calculated GMI.
• query-interval is the amount of time between general queries.

Values for the components in the GMI are obtained as follows:

• MRT is advertised in the general query, for both IGMPv2 and IGMPv3.

• If the querier is running IGMPv2, IGMP snooping uses the IGMP-snooping-configured values for the robustness-variable and query-interval. These parameter values must match the configured values for the querier. In most cases, if you are interacting with other Cisco routers, you should not need to explicitly configure these values—the default values for IGMP snooping should match the default values of the querier. If they do not, use the `querier robustness-variable` and `querier query-interval` commands to configure matching values.

• IGMPv3 general queries convey values for robustness-variable and query-interval (QRV and QQI, respectively). IGMP snooping uses the values from the query, making the IGMP snooping GMI exactly match that of the querier.

**Report Suppression (IGMPv2) and Proxy Reporting (IGMPv3)**

The following IGMP snooping features reduce multicast traffic in a bridge domain. Both are enabled by default.

• IGMPv2 report suppression—If the bridge domain querier is running IGMPv2, IGMP snooping suppresses joins from a host if it has already forwarded the same join from another host during the current query interval. IGMP snooping forwards the last leave message to all mrouter ports.

As insurance against lost reports when report suppression is enabled, IGMP snooping forwards IGMPv2 join reports the configured querier robustness-variable times for new groups. Configure the querier robustness-variable using the `querier robustness-variable` command.

• IGMPv3 proxy reporting—If the bridge domain querier is running IGMPv3, IGMP snooping acts as a proxy, generating reports from the proxy reporting address. Configure the proxy reporting address using the `system-ip-address` command. The default value is 0.0.0.0.

As insurance against lost reports when proxy reporting is enabled, IGMP snooping generates and forwards state change reports robustness-variable times, where the robustness-variable is the QRV value in the querier’s general query. The reports are forwarded at random intervals within the timeframe configured with the `unsolicited-report-timer` command.

To disable report suppression and proxy reporting, use the `report-suppression disable` command.

The scope for the commands mentioned in this section is the bridge domain. The commands are ignored in a profile attached to a port.

**Group Leave Processing**

**Group Leave Options**

When hosts want to leave a multicast group, they can either ignore the periodic general IGMP queries (called a silent leave), or they can send a group-specific leave message.

IGMP snooping can respond to group leaves in the following ways:

• Last member query processing—This is the default method for processing group leaves.
Immediate leave—You can optionally configure individual ports for immediate leave.

Note IGMPv3 explicit host tracking, which provides per host immediate leave functionality on a multi-host LAN, is not supported.

Last Member Query Processing for IGMPv2 and IGMPv3

Last member query is the default group leave processing method used by IGMP snooping. With last member query processing, IGMP snooping processes leave messages as follows:

- IGMP snooping sends group-specific queries on the port that receives the leave message to determine if any other devices connected to that interface are interested in traffic for the specified multicast group. Using the following two configuration commands, you can control the latency between the request for a leave and the actual leave:
  - `last-member-query-count` command—Controls the number of group-specific queries IGMP snooping sends in response to a leave message.
  - `last-member-query-interval` command—Controls the amount of time between group-specific queries.

- If IGMP snooping does not receive an IGMP join message in response to group-specific queries, it assumes that no other devices connected to the port are interested in receiving traffic for this multicast group, and it removes the port from its Layer-2 forwarding table entry for that multicast group.

- If the leave message was from the only remaining port, IGMP snooping removes the group entry and generates an IGMP leave to the multicast routers.

Immediate-Leave Configuration

Immediate-leave is an optional port-level configuration parameter. Immediate-leave processing causes IGMP snooping to remove a Layer-2 interface from the forwarding table entry immediately, without first sending IGMP group-specific queries to the interface. After receiving an IGMP leave message, IGMP snooping immediately removes the interface from the Layer-2 forwarding table entry for that multicast group, unless a multicast router was learned on the port.

Immediate-leave processing improves leave latency, but is appropriate only when one receiver is configured on a port. For example, immediate-leave is appropriate in the following situations:

- Point-to-point configurations, such as an IPTV channel receiver
- Downstream DSLAMs with proxy reporting

Do not use immediate-leave on a port when the possibility exists for more than one receiver per port. Doing so could prevent an interested receiver from receiving traffic. For example, immediate-leave is not appropriate in a LAN.

Immediate-leave processing is a port-level option. You can configure this option explicitly per port in port profiles or in the bridge domain profile, in which case, it applies to all ports under the bridge.
Reaction to Topology Change Notifications

In a Spanning Tree Protocol (STP) topology, a Topology Change Notification (TCN) indicates that an STP topology change has occurred. As a result of a topology change, m routers and hosts reporting group membership may migrate to other STP ports under the bridge domain. M router and membership states must be relearned after a TCN.

IGMP snooping reacts to TCNs in the following ways:

1. IGMP snooping temporarily extends the flood set for all known multicast routes to include all ports participating in STP that are in forwarding state. The short-term flooding ensures that multicast delivery continues to all m routers and all member hosts in the bridge domain while m router and membership states are relearned.

   But, as a result of this TCN flooding, downstream STP links may sometimes become over-subscribed by these extra multicast flows. This feature can in such cases be disabled by use of the tcn flood disable command.

2. The STP root bridge issues a global leave (for group 0.0.0.0) on all ports. This action triggers interoperable IGMP queriers to send general queries, expediting the relearning process.

   Sending global leaves for query solicitation is a Cisco-specific implementation.

Note 3. When the TCN refresh period ends, IGMP snooping withdraws the non-m router and non-member STP ports from the multicast route flood sets. You can control the amount of time that flooding occurs with the tcn flood query count command. This command sets the number of IGMP general queries for which the multicast traffic is flooded following a TCN, thereby influencing the refresh period.

IGMP snooping default behavior is that the STP root bridge always issues a global leave in response to a TCN, and that the non-root bridges do not issue global leaves.

With the tcn query solicit command, you can enable a bridge to always issue a global leave in response to TCNs, even when it is not the root bridge. In that case, the root bridge and the non-root bridge would issue the global leave and both would solicit general queries in response to a TCN. Use the no form of the command to turn off soliciting when the bridge is not the root.

Note One use for the tcn query solicit command is when Reverse Layer 2 Gateway Protocol (RL2GP) is configured to set up a MSTP Access Gateway. In this scenario, IGMP snooping is unaware of the root or non-root status of the bridge and, therefore, when a TCN occurs, no query is solicited in the domain unless IGMP snooping is explicitly configured to do so on at least one bridge.

The root bridge always issues a global leave in response to a TCN. This behavior cannot be disabled.

The internal querier has its own set of configuration options that control its reactions to TCNs.

The scope for all tcn related configuration option(s) is per bridge domain. If the command appears in profiles attached to ports, it has no effect.
**IGMP Snooping Packet Checks**

By default, IGMP snooping performs the following validations. If your network performs these validations elsewhere, you can disable the IGMP snooping validations.

- IGMP snooping checks the time-to-live (TTL) field in the IGMP header and drops packets where TTL is not equal to 1. The TTL field should always be set to 1 in the headers of IGMP reports and queries.
  
  You can disable this check using the `ttl-check disable` command, in which case IGMP snooping processes all packets without examining the TTL field in the IGMP header.

- IGMP snooping checks for the presence of the router alert option in the IP packet header of the IGMP message and drops packets that do not include this option.
  
  You can disable this check using the `router-alert-check disable` command, in which case IGMP snooping does not perform the validation before processing the message.

**Startup Query Configuration**

The startup query feature is configured using new igmp snooping profile parameters. You can configure the startup query processing in response to the following events:

- MC-LAG Port goes active
- Topology-change
- Port-up
- Process start

The above parameters are specific to MC-LAG feature. These are apart from the existing bridge domain level parameters such as count, MRT, and query interval. For more information about these CLI, refer the *Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference*.

**Note**

- For IGMP snooping to work on MC-LAG properly, the IGMP snooping configuration on both the POAs must be the same.

- In the case of downstream MC-LAG, when MC-LAG is configured and up and running, the MC-LAG port has to be added in IGMP Snooping enabled Bridge-domain.

- In the case of upstream MC-LAG, where POAs are attached to multicast router, the static mrouter port has to be configured on the multicast router that is towards both the POAs so that traffic is drawn to both the POAs.
IGMP Snooping Configuration at the Host Port Level

Router Guard and Static Mrouter

Router guard is a security feature that prevents malicious users from making a host port into an mrouter port. (This undesirable behavior is known as spoofing.) When a port is protected with the `router-guard` command, it cannot be dynamically discovered as an mrouter. When router guard is on a port, IGMP snooping filters protocol packets sent to the port and discards any that are multicast router control packets.

The `mrouter` command configures a port as a static mrouter.

You can use the `router-guard` and the `mrouter` commands on the same port to configure a guarded port as a static mrouter, for example, when:

- A large number of downstream host ports are present and you want to block dynamic mrouter discovery and configure static mrouters. In this case, configure the router guard feature at the domain level. By default, it will be applied to all ports, including the typically large number of downstream host ports. Then, use another profile without router guard configured for the relatively few upstream ports on which you want to permit dynamic mrouter discovery or configure static mrouters.

- Incompatibilities with non-Cisco equipment prevents correct dynamic discovery, you can disable all attempts for dynamic discovery using the router guard feature, and statically configure the mrouter.

If you are using the router guard feature, because there is an incompatible IGMP router on the port, you should also configure the `mrouter` command on the port to ensure that the router receives IGMP reports and multicast flows.

Immediate-Leave

See the Group Leave Processing, on page 11.

Static Groups

IGMP snooping learns Layer-2 multicast groups dynamically. You can also statically configure Layer-2 multicast groups.

You can use the `static group` command in profiles intended for bridge domains or ports. If you configure this option in a profile attached to a bridge domain, it applies to all ports under the bridge.

A profile can contain multiple static groups. You can define different source addresses for the same group address. Using the `source` keyword, you can configure IGMPv3 source groups.

Static group membership supersedes any dynamic manipulation by IGMP snooping. Multicast group membership lists can contain both static and dynamic group definitions.

When you configure a static group or source groups on a port, IGMP snooping adds the port as an outgoing port to the corresponding `<S/>G>` forwarding entry and sends an IGMPv2 join or IGMPv3 report to all mrouter ports. IGMP snooping continues to send the membership report in response to general queries for as long as the static group remains configured on the port.
Internal Querier

When to Use an Internal Querier

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier. In situations when no external querier exists in the bridge domain (because the multicast traffic does not need to be routed), but local multicast sources exist, you must configure an internal querier to implement IGMP snooping. The internal querier solicits membership reports from hosts in the bridge domain so that IGMP snooping can build constrained multicast forwarding tables for the multicast traffic within the bridge domain.

An internal querier might also be useful when interoperability issues with non-Cisco equipment prevent IGMP snooping from working correctly with an external querier. In this case, you can:

1. Prevent the uncooperative external querier from being discovered by placing the router-guard command on that port.
2. Configure an internal querier to learn group membership interests from the ports in the bridge domain.
3. Configure static mrouter ports to receive multicast traffic.

Internal Querier Default Configuration

The minimum configuration for an internal querier is:

- Add the `internal-querier` command to a profile attached to the bridge domain. The default configuration is shown in Table 4: Internal Querier Default Configuration Values, on page 16.
- Add the `system-ip-address` command to a profile attached to the bridge domain to configure an address other than the default 0.0.0.0.

<table>
<thead>
<tr>
<th>Configuration Command</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>system-ip-address</code></td>
<td>0.0.0.0. The default address is invalid for the internal-querier.</td>
</tr>
<tr>
<td><code>internal-querier max-response-time</code></td>
<td>10</td>
</tr>
<tr>
<td><code>internal-querier query-interval</code></td>
<td>60 (seconds)</td>
</tr>
<tr>
<td></td>
<td>Note: This is a nonstandard default value.</td>
</tr>
<tr>
<td><code>internal-querier robustness-variable</code></td>
<td>2</td>
</tr>
<tr>
<td><code>internal-querier tcn query count</code></td>
<td>2</td>
</tr>
<tr>
<td><code>internal-querier tcn query interval</code></td>
<td>10 (seconds)</td>
</tr>
</tbody>
</table>
You can disable the internal querier (using the no form of the `internal-querier` command) without removing any other internal querier commands. The additional internal querier commands are ignored in that case.

The scope for the `internal-querier` command is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

**Internal Querier Processing**

When the internal querier is the elected querier in the domain, it solicits membership reports by sending IGMP general queries at the interval specified by the `internal-querier query-interval` command on every active port in the bridge domain. The internal querier sends IGMPv3 queries by default. You can configure it to send IGMPv2 messages instead using the `internal-querier version` command.

The local IGMP snooping process responds to the internal querier's general queries. In particular, the IGMPv3 proxy (if enabled) generates a current-state report and forwards it to all mrouters. For IGMPv2 or when the IGMPv3 proxy is disabled, IGMP snooping generates current-state reports for static group state only.

The queries are sent from the address you configure for IGMP snooping using the `system-ip-address` command. The queries include the maximum response time configured with the `internal-querier max-response-time` command.

The `internal-querier robustness-variable` and `internal-querier query-interval` commands configure values for both IGMPv2 and IGMPv3 processing.

**Querier Election for One Active Querier**

A bridge domain can have only one active querier at a time. If the internal-querier receives queries from another querier in a bridge domain, it performs querier election. The lowest IP address wins. If the internal querier is the election loser, IGMP snooping starts a timer with the value set by the `internal-querier timer expiry` command. If this timer expires before another query is received from the election winner, the internal querier becomes the active querier.

The default `internal-querier timer expiry` command value is derived from the values of other configuration options, as described in Table 4: Internal Querier Default Configuration Values, on page 16. You can configure a different value to override the default calculation.
Internal Querier Reaction to TCNs

IGMP snooping generates group leaves in response to topology change notifications. For more information about how IGMP snooping reacts to TCNs, see the Reaction to Topology Change Notifications, on page 13.

If the internal querier receives a group leave while it is the elected querier in the domain, it reacts as follows:

- Generates an IGMP general query immediately.
- Waits the amount of time set by the `internal-querier tcn query interval` command and generates another IGMP general query.
- Continues to wait for the specified interval time and to send general queries until the query count reaches the value set with the `internal querier tcn query count` command.

**Note**
You can configure the internal querier to ignore global leaves by setting the internal querier TCN query count to 0.

How to Configure IGMP Snooping

The first two tasks are required to configure basic IGMP snooping configuration. The optional tasks configure additional IGMP snooping features and provide a way to view statistics and counters:

- Adding Static Mrouter Configuration to a Profile, on page 24 (optional)
- Adding Router Guard to a Profile, on page 25 (optional)
- Configuring Immediate-Leave, on page 27 (optional)
- Configuring Static Groups, on page 28 (optional)
- Configuring an Internal Querier, on page 29 (optional)
- Verifying Multicast Forwarding, on page 30 (optional)

Creating an IGMP Snooping Profile

**SUMMARY STEPS**

1. `configure`
2. `igmp snooping profile profile-name`
3. Optionally, add commands to override default configuration values.
4. `commit`
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> igmp snooping profile profile-name</td>
<td>Enters IGMP snooping profile configuration mode and creates a named profile. The default profile enables IGMP snooping. You can commit the new profile without any additional configurations, or you can include additional configuration options to the profile. You can also return to the profile later to add configurations, as described in other tasks in this module.</td>
</tr>
</tbody>
</table>
| **Step 3** Optionally, add commands to override default configuration values. | If you are creating a bridge domain profile, consider the following:  
  • An empty profile is appropriate for attaching to a bridge domain. An empty profile enables IGMP snooping with default configuration values.  
  • You can optionally add more commands to the profile to override default configuration values.  
  • If you include port-specific configurations in a bridge domain profile, the configurations apply to all ports under the bridge, unless another profile is attached to a port.  
  
  If you are creating a port-specific profile, consider the following:  
  • While an empty profile could be attached to a port, it would have no effect on the port configuration.  
  • When you attach a profile to a port, IGMP snooping reconfigures that port, overriding any inheritance of configuration values from the bridge-domain profile. You must repeat the commands in the port profile if you want to retain those configurations.  
  
  You can detach a profile, change it, and reattach it to add commands to a profile at a later time. |
| **Step 4** commit         |         |

**Where to Go Next**

You must attach a profile to a bridge domain or to a port to have it take effect. See one of the following tasks:

**Attaching a Profile and Activating IGMP Snooping on a Bridge Domain**

To activate IGMP snooping on a bridge domain, attach an IGMP snooping profile to the bridge domain, as described in the following steps.
### SUMMARY STEPS

1. configure
2. l2vpn
3. bridge group *bridge-group-name*
4. bridge-domain *bridge-domain-name*
5. igmp snooping profile *profile-name*
6. commit
7. show igmp snooping bridge-domain detail
8. show l2vpn bridge-domain detail

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters Layer 2 VPN configuration mode.</td>
</tr>
<tr>
<td>Step 2 l2vpn</td>
<td>Enters Layer 2 VPN VPLS bridge group configuration mode for the named bridge group.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# l2vpn</td>
</tr>
<tr>
<td>Step 3 bridge group <em>bridge-group-name</em></td>
<td>Enters Layer 2 VPN VPLS bridge group bridge domain configuration mode for the named bridge domain.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1</td>
</tr>
<tr>
<td>Step 4 bridge-domain <em>bridge-domain-name</em></td>
<td>Attaches the named IGMP snooping profile to the bridge domain, enabling IGMP snooping on the bridge domain.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1</td>
</tr>
<tr>
<td>Step 5 igmp snooping profile <em>profile-name</em></td>
<td>(Optional) Verifies that IGMP snooping is enabled on a bridge domain and shows the IGMP snooping profile names attached to bridge domains and ports.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router# show igmp snooping</td>
</tr>
</tbody>
</table>
Detaching a Profile and Deactivating IGMP Snooping on a Bridge Domain

To deactivate IGMP snooping on a bridge domain, remove the profile from the bridge domain using the following steps.

**Note**

A bridge domain can have only one profile attached to it at a time.

**SUMMARY STEPS**

1. configure
2. l2vpn
3. bridge group `bridge-group-name`
4. bridge-domain `bridge-domain-name`
5. no igmp snooping
6. commit
7. show igmp snooping bridge-domain detail
8. show l2vpn bridge-domain detail

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>l2vpn</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config)# l2vpn
```
### Attaching and Detaching Profiles to Ports Under a Bridge

#### Before You Begin

IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>bridge group bridge-group-name</code></td>
<td>Enters Layer 2 VPN VPLS bridge group configuration mode for the named bridge group.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1</code></td>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 4</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bridge-domain bridge-domain-name</code></td>
<td>Enters Layer 2 VPN VPLS bridge group bridge domain configuration mode for the named bridge domain.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1</code></td>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 5</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no igmp snooping</code></td>
<td>Detaches the IGMP snooping profile from the bridge domain, disabling IGMP snooping on that bridge domain.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Only one profile can be attached to a bridge domain at a time. If a profile is attached, IGMP snooping is enabled. If a profile is not attached, IGMP snooping is disabled.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# no igmp snooping</code></td>
<td><code>RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# no igmp snooping</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 6</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>commit</code></td>
<td>(Optional) Verifies that IGMP snooping is disabled on a bridge domain.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 7</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show igmp snooping bridge-domain detail</code></td>
<td>(Optional) Verifies that IGMP snooping is disabled in the forwarding plane (Layer 2) on a bridge domain.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router# show igmp snooping bridge-domain detail</code></td>
<td><code>RP/0/RSP0/CPU0:router# show igmp snooping bridge-domain detail</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Step 8</strong></th>
<th><strong>Purpose</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show l2vpn bridge-domain detail</code></td>
<td>(Optional) Verifies that IGMP snooping is disabled in the forwarding plane (Layer 2) on a bridge domain.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router# show l2vpn bridge-domain</code></td>
<td><code>RP/0/RSP0/CPU0:router# show l2vpn bridge-domain</code></td>
</tr>
</tbody>
</table>
SUMMARY STEPS

1. configure
2. l2vpn
3. bridge group bridge-group-name
4. bridge-domain bridge-domain-name
5. interface interface-type interface-number
6. Do one of the following:
   • igmp snooping profile profile-name
   • no igmp snooping
7. commit
8. show igmp snooping bridge-domain detail
9. show l2vpn bridge-domain detail

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure En ters Layer 2 VPN configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>l2vpn     Enters Layer 2 VPN configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# l2vpn</td>
</tr>
<tr>
<td>Step 3</td>
<td>bridge group bridge-group-name Enters Layer 2 VPN bridge group configuration mode for the named bridge group.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1</td>
</tr>
<tr>
<td>Step 4</td>
<td>bridge-domain bridge-domain-name Enters Layer 2 VPN bridge group bridge domain configuration mode for the named bridge domain.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1</td>
</tr>
<tr>
<td>Step 5</td>
<td>interface interface-type interface-number Enters Layer 2 VPN VPLS bridge group bridge domain interface configuration mode for the named interface or PW.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface gig 1/1/1/1</td>
</tr>
<tr>
<td>Step 6</td>
<td>Do one of the following: Attaches the named IGMP snooping profile to the port.</td>
</tr>
</tbody>
</table>
Adding Static Mrouter Configuration to a Profile

Before You Begin
IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

Note: Static mrouter port configuration is a port-level option and should be added to profiles intended for ports. It is not recommended to add mrouter port configuration to a profile intended for bridge domains.

SUMMARY STEPS

1. configure
2. igmp snooping profile profile-name
3. mrouter
4. commit
5. show igmp snooping profile profile-name detail
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> igmp snooping profile <em>profile-name</em></td>
<td>Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# igmp snooping profile mrouter-port-profile</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mrouter</td>
<td>Configures a port as a static mrouter port.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# mrouter</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> commit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> show igmp snooping profile <em>profile-name</em> detail</td>
<td>(Optional) Displays the configuration settings in the named profile.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# show igmp snooping profile mrouter-port-profile detail</td>
<td></td>
</tr>
</tbody>
</table>

### Where to Go Next

Attach the profile to ports to complete static mrouter configuration. See the [Attaching and Detaching Profiles to Ports Under a Bridge](#), on page 22.

### Adding Router Guard to a Profile

To prevent multicast routing protocol messages from being received on a port and, therefore, prevent a port from being a dynamic mrouter port, follow these steps. Note that both router guard and static mrouter commands may be configured on the same port. See the [Router Guard and Static Mrouter](#), on page 15 for information.

### Before You Begin

IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.
Routerguardconfigurationisaport-leveloptionandshouldbeaddedtoprofilesintendedforports. It is not recommended toaddrouterguardconfigurationtoaprofileintendedforbridgedomains. Todoso would preven tallmrouters, includingIGMPqueriers, frombeingdiscoveredinthebridgedomain.

**SUMMARY STEPS**

1. configure
2. igmp snooping profile *profile-name*
3. router-guard
4. commit
5. show igmp snooping profile *profile-name* detail

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 2** igmp snooping profile *profile-name*  
Example:  
RP/0/RSP0/CPU0:router(config)# igmp snooping profile host-port-profile | Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile. |
| **Step 3** router-guard  
Example:  
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# router-guard | Protects the port from dynamic discovery. |
| **Step 4** commit | |
| **Step 5** show igmp snooping profile *profile-name* detail  
Example:  
RP/0/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail | (Optional) Displays the configuration settings in the named profile. |

**Where to Go Next**

Attach the profile to ports to complete router guard configuration. See the Attaching and Detaching Profiles to Ports Under a Bridge, on page 22.
Configuring Immediate-Leave

To add the IGMP snooping immediate-leave option to an IGMP snooping profile, follow these steps.

Before You Begin
IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

SUMMARY STEPS

1. configure
2. igmp snooping profile profile-name
3. immediate-leave
4. commit
5. show igmp snooping profile profile-name detail

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.</td>
</tr>
<tr>
<td>Step 2</td>
<td>igmp snooping profile profile-name</td>
<td>Enables the immediate-leave option.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/O/RSP0/CPU0:router(config)# igmp snooping profile host-port-profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>immediate-leave</td>
<td>Enables the immediate-leave option.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/O/RSP0/CPU0:router(config-igmp-snooping-profile)# immediate-leave</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you add this option to a profile attached to a bridge domain, it applies to all ports under the bridge.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If you add this option to a profile attached to a port, it applies to the port.</td>
</tr>
<tr>
<td>Step 4</td>
<td>commit</td>
<td>(Optional) Displays the configuration settings in the named profile.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show igmp snooping profile profile-name detail</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/O/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Where to Go Next

Attach the profile to bridge domains or ports to complete immediate-leave configuration. See one of the following sections:

Configuring Static Groups

To add one or more static groups or IGMPv3 source groups to an IGMP snooping profile, follow these steps.

Before You Begin

IGMP snooping must be enabled on the bridge domain for port-specific profiles to affect IGMP snooping behavior.

SUMMARY STEPS

1. configure
2. igmp snooping profile profile-name
3. static-group group-addr [source source-addr]
4. Repeat the previous step, as needed, to add more static groups.
5. commit
6. show igmp snooping profile profile-name detail

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.</td>
</tr>
<tr>
<td>Step 2 igmp snooping profile profile-name</td>
<td></td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# igmp snooping profile host-port-profile</td>
<td></td>
</tr>
<tr>
<td>Step 3 static-group group-addr [source source-addr]</td>
<td>Configures a static group.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# static-group 239.1.1.1 source 10.0.1.1</td>
<td></td>
</tr>
<tr>
<td>Step 4 Repeat the previous step, as needed, to add more static groups.</td>
<td>(Optional) Adds additional static groups.</td>
</tr>
<tr>
<td>Step 5 commit</td>
<td></td>
</tr>
</tbody>
</table>
**Implementing Layer-2 Multicast with IGMP Snooping**

**Configuring an Internal Querier**

**Before You Begin**

IGMP snooping must be enabled on the bridge domain for this procedure to take effect.

**SUMMARY STEPS**

1. configure
2. `igmp snooping profile profile-name`
3. system-ip-address `ip-addr`
4. internal-querier
5. commit
6. show igmp snooping profile `profile-name` detail

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.</td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>igmp snooping profile profile-name</code></td>
<td>(Optional) Displays the configuration settings in the named profile.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router# show igmp snooping profile host-port-profile detail
```

**Where to Go Next**

Attach the profile to bridge domains or ports to complete static-group configuration. See one of the following sections:

**Configuring an Internal Querier**
Verifying Multicast Forwarding

SUMMARY STEPS

1. configure
2. show 12vpn forwarding bridge-domain [bridge-group-name:bridge-domain-name] mroute ipv4 [detail] [hardware {ingress | egress}] location node-id
3. show 12vpn forwarding bridge-domain [bridge-group-name:bridge-domain-name] mroute ipv4 summary location node-id

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Group Limits

This procedure consists the following tasks:

#### Configuring route-policy

**SUMMARY STEPS**

1. configure
2. route-policy *policy-name*
3. end-policy
4. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring group limits

#### SUMMARY STEPS

1. `configure`
2. `igmp snooping profile profile-name`
3. `group policy policy-name`
4. `group limit range`
5. `commit`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enters IGMP snooping profile configuration mode and creates a new profile or accesses an existing profile.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>igmp snooping profile profile-name</code></td>
<td>Specifies the configured route-policy to set the group weight.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# igmp snooping profile name1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>group policy policy-name</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# group policy policy1</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring access-groups

This task instructs IGMP Snoop to apply the specified access-list filter(s) to receive membership reports. The user needs to create and configure access-lists before configuring the access-groups. For detailed configuration procedures, for creating and configuring standard and extended access-lists, refer to the Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide.

**SUMMARY STEPS**

1. configure
2. `igmp snooping profile profile-name`
3. `access-group acl-name`
4. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>igmp snooping profile profile-name</code></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# igmp snooping profile name1</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>access-group acl-name</code></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# access-group acl1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# group limit 100
```
Configuration Examples for IGMP Snooping

The following examples show how to enable IGMP snooping on Layer 2 VPLS bridge domains on Cisco ASR 9000 Series Routers:

Configuring IGMP Snooping on Physical Interfaces Under a Bridge: Example

1. Create two profiles.

   igmp snooping profile bridge_profile
   !
   igmp snooping profile port_profile
     mrouter
     !

2. Configure two physical interfaces for L2 transport.

   interface GigabitEthernet0/8/0/38
     negotiation auto
     l2transport
     no shut
     !
   !
   interface GigabitEthernet0/8/0/39
     negotiation auto
     l2transport
     no shut
     !
   !

3. Add interfaces to the bridge domain. Attach bridge_profile to the bridge domain and port_profile to one of the Ethernet interfaces. The second Ethernet interface inherits IGMP snooping configuration attributes from the bridge domain profile.

   l2vpn
     bridge group bg1
     bridge-domain bd1
     igmp snooping profile bridge_profile
     interface GigabitEthernet0/8/0/38
     igmp snooping profile port_profile
     interface GigabitEthernet0/8/0/39
     !
     !

4. Verify the configured bridge ports.

   show igmp snooping port
Configuring IGMP Snooping on VLAN Interfaces Under a Bridge: Example

1 Configure two profiles.

```configuration
igmp snooping profile bridge_profile
igmp snooping profile port_profile
mrouter !
```

2 Configure VLAN interfaces for L2 transport.

```configuration
interface GigabitEthernet0/8/0/8
   negotiation auto
   no shut
!
interface GigabitEthernet0/8/0/8.1 l2transport
   encapsulation dot1q 1001
   mtu 1514
!
interface GigabitEthernet0/8/0/8.2 l2transport
   encapsulation dot1q 1002
   mtu 1514
!
```

3 Attach a profile and add interfaces to the bridge domain. Attach a profile to one of the interfaces. The other interface inherits IGMP snooping configuration attributes from the bridge domain profile.

```configuration
l2vpn
   bridge group bg1
   bridge-domain bd1
   igmp snooping profile bridge_profile
   interface GigabitEthernet0/8/0/8.1
      igmp snooping profile port_profile
   interface GigabitEthernet0/8/0/8.2
!
!
```

4 Verify the configured bridge ports.

```configuration
show igmp snooping port
```

Configuring IGMP Snooping on Ethernet Bundles Under a Bridge: Example

1 This example assumes that the front-ends of the bundles are preconfigured. For example, a bundle configuration might consist of three switch interfaces, as follows:

```configuration
interface Port-channel1
!
interface GigabitEthernet0/0/0/0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/2
   channel-group 1 mode on
!
interface GigabitEthernet0/0/0/3
```
channel-group 1 mode on

1 Configure two IGMP snooping profiles.

```plaintext
ingmp snooping profile bridge_profile
  igmp snooping profile port_profile
  mrouterr
```

2 Configure interfaces as bundle member links.

```plaintext
interface GigabitEthernet0/0/0/0
  bundle id 1 mode on
  negotiation auto

interface GigabitEthernet0/0/0/1
  bundle id 1 mode on
  negotiation auto

interface GigabitEthernet0/0/0/2
  bundle id 2 mode on
  negotiation auto

interface GigabitEthernet0/0/0/3
  bundle id 2 mode on
  negotiation auto
```

3 Configure the bundle interfaces for L2 transport.

```plaintext
interface Bundle-Ether 1
  l2transport

interface Bundle-Ether 2
  l2transport
```

4 Add the interfaces to the bridge domain and attach IGMP snooping profiles.

```plaintext
l2vpn
  bridge group bg1
  bridge-domain bd1
  igmp snooping profile bridge_profile
  interface Bundle-Ether 1
  igmp snooping profile port_profile
  interface Bundle-Ether 2
```

5 Verify the configured bridge ports.

```plaintext
show igmp snooping port
```
Configuring IGMP Snooping on VFIs Under a Bridge: Example

This example configures IGMP snooping on a virtual forwarding instance (VFI) under a bridge domain. The topology consists of two routers, PE1 and PE2, each with an access circuit (AC) and pseudowire (PW) as bridge ports.

PE1 Configuration

1. Configure IGMP snooping profiles.

   ```
   igmp snooping profile prof1
   !
   igmp snooping profile prof2
   mrouter
   !
   ```

2. Configure interfaces.

   ```
   interface Loopback0
     ipv4 address 10.1.1.1 255.255.255.255
   !
   interface GigabitEthernet0/2/0/9
     ipv4 address 10.10.10.1 255.255.255.0
     negotiation auto
   !
   interface GigabitEthernet0/2/0/39
     negotiation auto
     l2transport
   !
   ```

3. Configure Open Shortest Path First (OSPF).

   ```
   router ospf 1
     log adjacency changes
     router-id 10.1.1.1
     area 0
     interface Loopback0
     !
     interface GigabitEthernet0/2/0/9
     !
   ```


   ```
   mpls ldp
     router-id 10.1.1.1
     log neighbor
     !
     interface GigabitEthernet0/2/0/9
     !
   ```

5. Configure a bridge domain, enable IGMP snooping on the bridge, and add the interfaces to the bridge domain.

   ```
   l2vpn
     pw-class atom-dyn
   ```
bridge group bg1
  bridge-domain bd1
  igmp snooping profile prof1
  interface GigabitEthernet0/2/0/39
    igmp snooping profile prof2
    vfi mplscore
      neighbor 10.2.2.2 pw-id 101
      pw-class atom-dyn
    !
    !

6 Verify the configured bridge ports.

  show igmp snooping port

PE2 Configuration

1 Configure the IGMP profiles.

  igmp snooping profile bridge_profile
  !
  igmp snooping profile port_profile
    mrouter
    !

2 Configure interfaces.

  interface Loopback0
    ipv4 address 10.2.2.2 255.255.255.255
    !
  interface GigabitEthernet0/2/0/9
    ipv4 address 10.10.10.1 255.255.255.0
    negotiation auto
    !
  interface GigabitEthernet0/2/0/39
    negotiation auto
    l2transport
    !

3 Configure OSPF.

  router ospf 1
    log adjacency changes
    router-id 10.2.2.2
    area 0
      interface Loopback0
      !
      interface GigabitEthernet0/2/0/9
      !
    !

4 Configure LDP.

  mpls ldp
    router-id 10.2.2.2
    log neighbor
    !
    interface GigabitEthernet0/2/0/9
    !
5 Add interfaces to the bridge domain and attach IGMP snooping profiles.

```snmp
l2vpn
   pw-class atom-dyn
   encapsulation mpls
   protocol ldp
!
!
bridge group bg1
   bridge-domain bd1
   igmp snooping profile bridge_profile
   interface GigabitEthernet0/2/0/39
   igmp snooping profile port_profile
   vfi mplscore
   neighbor 10.1.1.1 pw-id 101
   pw-class atom-dyn
!
!
```

6 Verify the configured bridge ports.

```bash
show igmp snooping port
```

**Configuring IGMP access-groups**

In the example below, a list is configured and attached to an L2VPN bridge port that allows user membership of `<*,G>` groups 225.0.0.0/24 and 228.0.0.0/24, only. A second access-list is defined that permits `<S,G>` membership. This access-list is attached to a bridge-port.

```bash
interface gig 0/2/0/1.1 l2transport
...
!
ipv4 access-list iptv-basic-white-list
  10 permit ipv4 any 225.0.0.0/24
  20 permit ipv4 any 228.0.0.0/24
!
ipv4 access-list iptv-premium-white-list
  10 permit ipv4 192.168.0.1 232.0.1.0/24
  20 permit ipv4 192.168.0.1 232.0.2.0/24
!
igmp snooping profile iptv
   access-group iptv-white-list
!
igmp snooping profile iptv2
   access-group iptv-premium-white-list
!
l2vpn
   bridge group vz
   bridge domain vz-liptv
   igmp snooping profile iptv
   interface gig 0/2/0/1.1
   interface gig 0/2/0/1.2
   igmp snooping profile iptv2
   interface gig 0/2/0/1.3
   ...
!
```

IGMP routing also supports access-groups using the `igmp access-group` command. It uses simple IP access-groups to specify group address filters. In order to support source-group filters as well as group filters, IGMP Snooping requires extended IP access-lists.
Note

Access-groups are not applied to static groups and source-groups.

Configuring IGMP Snooping over MCLAG: Example

Case 1: Downstream MCLAG

Topology: DHD connected to 2 POAs which in turn is connected to PE.

DHD:

1. Configure a bundle towards POA1 and POA2. This device will be masked from the existence of 2 POAs. The bundle considers that it is connected to a single POA.

   ```
   interface Bundle-Ether10
   description interface towards POAs
   lacp switchover suppress-flaps 100
   bundle maximum-active links 1
   l2transport
   
   !
   
   interface GigabitEthernet0/0/0/28
   description interface towards POA1
   bundle id 10 mode active
   
   !
   
   interface GigabitEthernet0/0/0/29
   description interface towards POA2
   bundle id 10 mode active
   ```

2. Joins coming to this must be forwarded to POAs over bundle. So, configuring the incoming port (host port) and bundle in L2VPN BD (without snooping).

   ```
   RP/0/RSP0/CPU0:router:DHD# show running-config l2vpn
   l2vpn
   bridge group bg1
   bridge-domain bg1_bd1
   interface Bundle-Ether10
   
   !
   interface GigabitEthernet0/0/0/10
   !
   ```
POA1:

1 Configure interfaces (for OSPF and MPLS LDP)

   interface Loopback0
   ipv4 address 20.20.20.20 255.255.255.255
   !
   interface GigabitEthernet0/2/0/1
description interface towards POA2
   ipv4 address 10.0.0.1 255.255.255.0
   negotiation auto
   !
   interface GigabitEthernet0/2/0/8
description interface towards PE
   ipv4 address 10.0.1.1 255.255.255.0
   negotiation auto
   !

2 Configure OSPF and MPLS LDP:

   router ospf 1
   router-id 20.20.20.20
   nsf cisco
   area 0
   interface Loopback0
   !
   interface GigabitEthernet0/2/0/1
   !
   interface GigabitEthernet0/2/0/8
   !

   !
   mpls ldp
   router-id 20.20.20.20
   graceful-restart
   interface GigabitEthernet0/2/0/1
   !
   interface GigabitEthernet0/2/0/8
   !

   !

3 Configure an MCLAG bundle towards DHD:

   interface Bundle-Ether10
   description interface towards DHD
   lacp switchover suppress-flaps 100
   mlacp iccp-group 1
   mlacp switchover recovery-delay 60
   mlacp port-priority 1
   mac-address 0.aaaa.1111
   bundle wait-while 0
   l2transport
interface GigabitEthernet0/2/0/29
bundle id 10 mode active

4 Configure redundancy group for MCLAG:

redundancy
  iccp
  group 1
  mlacp node 1
  mlacp system mac 0000.aaaa.0000
  mlacp system priority 1
  member
  neighbor 30.30.30.30
  !
  backbone
  interface GigabitEthernet0/2/0/8
  !
  !

5 Configure IGMP Snooping profile:

  igmp snooping profile p1
  ttl-check disable
  router-alert-check disable
  !

6 Enable IGMP Snooping in the L2VPN BD which includes MCLAG bundle towards DHD and PW towards PE:

  l2vpn
  bridge group bg1
  bridge-domain bg1_bd1
  igmp snooping profile p1
  interface Bundle-Ether10
  !
  vfi bg1_bd1_vfi
  neighbor 40.40.40.40 pw-id 1
  !
  !
  !

POA2:

1 Configure interfaces (for OSPF and MPLS LDP)

  interface Loopback0
  ipv4 address 30.30.30.30 255.255.255.255
interface GigabitEthernet0/0/0/1
description interface towards POA1
ipv4 address 10.0.0.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/8
description interface towards PE
ipv4 address 10.0.2.1 255.255.255.0
negotiation auto
!

2  Configure OSPF and MPLS LDP:

    router ospf 1
    router-id 30.30.30.30
    nsf cisco
    area 0
    interface Loopback0
    !
    interface GigabitEthernet0/0/0/1
    !
    interface GigabitEthernet0/0/0/8
    !
    !
    mpls ldp
    router-id 30.30.30.30
    graceful-restart
    interface GigabitEthernet0/0/0/1
    !
    interface GigabitEthernet0/0/0/8
    !
    !

3  Configure an MCLAG bundle towards DHD:

    interface Bundle-Ether10
    description interface towards DHD
    lacp switchover suppress-flaps 100
    mlacp iccp-group 1
    mlacp switchover recovery-delay 60
    mlacp port-priority 2
    mac-address 0.aaaa.1111
    bundle wait-while 0
    l2transport
    !
    !
    interface GigabitEthernet0/0/0/28
    bundle id 10 mode active
    !

4  Configure redundancy group for MCLAG:

    redundancy
    iccp
    group 1
    mlacp node 2
    mlacp system mac 0000.aaaa.0000
    mlacp system priority 1
    member
    neighbor 20.20.20.20
    !
    backbone
5 Configure IGMP Snooping profile:

```
igmp snooping profile p1
ttl-check disable
router-alert-check disable
```

6 Enable IGMP Snooping in the L2VPN BD which includes MCLAG bundle towards DHD and PW towards PE:

```
l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface Bundle-Ether10
  vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1
```

PE:

1 Configure Interfaces:

```
interface Loopback0
  ipv4 address 40.40.40.40 255.255.255.255
  !
interface GigabitEthernet0/0/0/8
description interface towards POA1
  ipv4 address 10.0.1.2 255.255.255.0
  negotiation auto
  !
interface GigabitEthernet0/0/0/9
description interface towards POA2
  ipv4 address 10.0.2.2 255.255.255.0
  negotiation auto
  !
interface GigabitEthernet0/0/0/20
description interface towards Multicast Router
  l2transport
  !
```

2 Configure OSPF and MPLS LDP:

```
router ospf 1
  router-id 40.40.40.40
  nsf cisco
  area 0
  interface Loopback0
  !
```
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
mls ldp
router-id 40.40.40.40
graceful-restart

interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!

3 Configure IGMP Snooping profile:

igmp snooping profile p1
ttl-check disable
router-alert-check disable
!

4 Enable IGMP Snooping in the L2VPN BD which includes PWs towards both the POAs and a port towards Multicast Router:

l2vpn
bridge group bg1
bridge-domain bg1_bd1
igmp snooping profile p1
interface GigabitEthernet0/0/0/20
!
vfi bg1_bd1_vfi
neighbor 20.20.20.20 pw-id 1
!
neighbor 30.30.30.30 pw-id 1
!
!

Case 2 : Upstream MCLAG

Topology: The multicast router is connected to 2 POAs and which is in turn connected to PE multicast Router.

1 Configure bundle towards POAs.

interface Bundle-Ether10
description interface towards POAs
ipv4 address 100.0.0.1 255.255.255.0
lacp switchover suppress-flaps 100
bundle maximum-active links 1
!
interface GigabitEthernet0/0/0/28
description interface towards POA1
bundle id 10 mode active
!
interface GigabitEthernet0/0/0/29
description interface towards POA2
bundle id 10 mode active
!

2 Enable multicast routing on the bundle interface:

multicast-routing
address-family ipv4
interface Bundle-Ether10
POA1:

1 Configure interfaces (for OSPF and MPLS LDP).

```
interface Loopback0
ipv4 address 20.20.20.20 255.255.255.255
!
interface GigabitEthernet0/2/0/1
description interface towards POA2
ipv4 address 10.0.0.1 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/2/0/8
description interface towards PE
ipv4 address 10.0.1.1 255.255.255.0
negotiation auto
!
```

2 Configure OSPF and MPLS LDP:

```
router ospf 1
router-id 20.20.20.20
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/2/0/1
!
interface GigabitEthernet0/2/0/8
!
!
mpls ldp
router-id 20.20.20.20
graceful-restart
interface GigabitEthernet0/2/0/1
!
interface GigabitEthernet0/2/0/8
!
!
```

3 Configure an MCLAG bundle towards DHD:

```
interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 1
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport
!
!
interface GigabitEthernet0/2/0/29
bundle id 10 mode active
!
```

4 Configure redundancy group for MCLAG:

```
redundancy
```
Configure IGMP Snooping profile:

```
igmp snooping profile p1
  ttl-check disable
  router-alert-check disable
```

6 Enable IGMP Snooping in the L2VPN BD which includes MCLAG bundle towards DHD and PW towards PE:

```
l2vpn
  bridge group bg1
  bridge-domain bg1_bd1
  igmp snooping profile p1
  interface Bundle-Ether10
  vfi bg1_bd1_vfi
  neighbor 40.40.40.40 pw-id 1
```

POA2:

1 Configure interfaces (for OSPF and MPLS LDP):

```
interface Loopback0
  ipv4 address 30.30.30.30 255.255.255.255

interface GigabitEthernet0/0/0/1
  description interface towards POA1
  ipv4 address 10.0.0.2 255.255.255.0
  negotiation auto

interface GigabitEthernet0/0/0/8
  description interface towards PE
  ipv4 address 10.0.2.1 255.255.255.0
  negotiation auto
```

2 Configure OSPF and MPLS LDP:

```
router ospf 1
  router-id 30.30.30.30
  nsf cisco
  area 0
  interface Loopback0
  !
  interface GigabitEthernet0/0/0/1
  !
  interface GigabitEthernet0/0/0/8
```
mpls ldp
router-id 30.30.30.30
graceful-restart
interface GigabitEthernet0/0/0/1
! interface GigabitEthernet0/0/0/8
!

3 Configure an MCLAG bundle towards DHD:

interface Bundle-Ether10
description interface towards DHD
lacp switchover suppress-flaps 100
mlacp iccp-group 1
mlacp switchover recovery-delay 60
mlacp port-priority 2
mac-address 0.aaaa.1111
bundle wait-while 0
l2transport
!
interface GigabitEthernet0/0/0/28
bundle id 10 mode active
!

4 Configure redundancy group for MCLAG:

redundancy
iccp
group 1
mlacp node 2
mlacp system mac 0000.aaaa.0000
mlacp system priority 1
member
neighbor 20.20.20.20
!
backbone
interface GigabitEthernet0/0/0/8
!
!

5 Configure IGMP Snooping profile:

igmp snooping profile p1
ttl-check disable
router-alert-check disable
!

6 Enable IGMP Snooping in the L2VPN BD which includes MCLAG bundle towards DHD and PW towards PE:

l2vpn
bridge group bg1
bridge-domain bg1 bd1
igmp snooping profile p1
interface Bundle-Ether10
!
vfi bg1_bd1_vfi
neighbor 40.40.40.40 pw-id 1
!
!
PE:

1 Configure interfaces:

```plaintext
interface Loopback0
ipv4 address 40.40.40.40 255.255.255.255
!
interface GigabitEthernet0/0/0/8
description interface towards POA1
ipv4 address 10.0.1.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/9
description interface towards POA2
ipv4 address 10.0.2.2 255.255.255.0
negotiation auto
!
interface GigabitEthernet0/0/0/20
description interface towards Host
l2transport
```

2 Configure OSPF and MPLS LDP:

```plaintext
router ospf 1
router-id 40.40.40.40
nsf cisco
area 0
interface Loopback0
!
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
mpls ldp
router-id 40.40.40.40
graceful-restart
interface GigabitEthernet0/0/0/8
!
interface GigabitEthernet0/0/0/9
!
!
```

3 Configure IGMP Snooping profile:

```plaintext
igmp snooping profile p1
ttl-check disable
router-alert-check disable
!
igmp snooping profile p2
mrouter
```

4 Enable IGMP Snooping in the L2VPN BD which includes PWs towards both the POAs and a port towards the Host. Configure static mrouter port on the PWs towards both the POAs.

```plaintext
l2vpn
bridge group bg1
bridge-domain bg1 bd1
igmp snooping profile p1
interface GigabitEthernet0/0/0/20
!
vfi bg1 bd1_vfi
neighbor 20.20.20.20 pw-id 1
igmp snooping profile p2
!```
neighbor 30.30.30.30 pw-id 1
igmp snooping profile p2
!
!
!
!

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring MPLS VPLS bridges</td>
<td>Implementing Virtual Private LAN Services on Cisco IOS XR Software module in the Cisco ASR 9000 Series Aggregation Services Router MPLS Configuration Guide</td>
</tr>
<tr>
<td>Getting started information</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</td>
</tr>
<tr>
<td>Configuring EFPs and EFP bundles</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide</td>
</tr>
</tbody>
</table>

Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>

1 Not all supported standards are listed.

MIBs

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>No MIBs support IGMP snooping.</td>
<td>To locate and download MIBs using Cisco IOS XR software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: <a href="http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a></td>
</tr>
</tbody>
</table>
### RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC-4541</td>
<td>Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Implementing Layer-3 Multicast Routing on Cisco IOS XR Software

This module describes how to implement Layer 3 multicast routing on Cisco ASR 9000 Series Routers running Cisco IOS XR Software.

**Multicast routing** is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients and homes. Applications that take advantage of multicast routing include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

This document assumes that you are familiar with IPv4 and IPv6 multicast routing configuration tasks and concepts for Cisco IOS XR Software.

Multicast routing allows a host to send packets to a subset of all hosts as a group transmission rather than to a single host, as in unicast transmission, or to all hosts, as in broadcast transmission. The subset of hosts is known as **group members** and are identified by a single multicast group address that falls under the IP Class D address range from 224.0.0.0 through 239.255.255.255.

For detailed conceptual information about multicast routing and complete descriptions of the multicast routing commands listed in this module, you can refer to the **Related Documents**, on page 237.

### Feature History for Configuring Multicast Routing on the Cisco ASR 9000 Series Routers

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>
| Release 3.9.0 | Support was added for these features:  
- Flow-based multicast only fast reroute (MoFRR).  
- IGMP VRF override. |
<p>| Release 3.9.1 | Support was added for the Multicast VPN feature. (For IPv4 address family) |</p>
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>Support was added for IPv4 Multicast routing, Multicast VPN basic and InterAS option A on Cisco ASR 9000 Series SPA Interface Processor-700 linecard and MVPN Hub and Spoke Topology.</td>
</tr>
<tr>
<td>Release 4.0.1</td>
<td>Support was added for IPv6 Multicast routing.</td>
</tr>
<tr>
<td>Release 4.1.0</td>
<td>Support was added for Label Switched Multicast using Point-to-Multipoint Traffic Engineering in global context only (not in VRF).</td>
</tr>
<tr>
<td>Release 4.2.1</td>
<td>Support was added for these features:</td>
</tr>
<tr>
<td></td>
<td>• Label Switched Multicast using MLDP (Multicast Label Distribution Protocol).</td>
</tr>
<tr>
<td></td>
<td>• Multicast VPN for IPv6 address family.</td>
</tr>
<tr>
<td></td>
<td>• Support for Satellite nV.</td>
</tr>
<tr>
<td></td>
<td>• InterAS Support on Multicast VPN.</td>
</tr>
<tr>
<td>Release 4.3.2</td>
<td>Support was added for these features:</td>
</tr>
<tr>
<td></td>
<td>• Support for IPv4 traffic on Multicast over unicast GRE was introduced.</td>
</tr>
<tr>
<td></td>
<td>• Support was added for TI (Topology Independent) MoFRR.</td>
</tr>
<tr>
<td>Release 5.2.0</td>
<td>Support was introduced for Bidirectional Global Protocol Independent Multicast.</td>
</tr>
<tr>
<td>Release 6.1.1</td>
<td>Layer 3 Multicast Bundle Subinterface Load Balancing feature was introduced.</td>
</tr>
<tr>
<td>Release 6.1.1</td>
<td>Segmented Multicast Stitching with Inter AS and MLDP Carrier Supporting Carrier based MVPN feature support was extended to support Cisco IOS XR 64 bit.</td>
</tr>
<tr>
<td>Release 6.1.1</td>
<td>MVPN, MoGRE, MoFRR and Global Table Multicast feature support was extended to support Cisco IOS XR 64 bit.</td>
</tr>
</tbody>
</table>

- Prerequisites for Implementing Multicast Routing, page 55
- Information About Implementing Multicast Routing, page 55
- How to Implement Multicast Routing, page 102
- Multicast only fast reroute (MoFRR), page 171
- Configuring Route Policy for Static RPF, page 175
Prerequisites for Implementing Multicast Routing

- You must install and activate the multicast pie.
- For detailed information about optional PIE installation, see *Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide*
- For MLDP, an MPLS PIE has to be installed.
- You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
- You must be familiar with IPv4 and IPv6 multicast routing configuration tasks and concepts.
- Unicast routing must be operational.
- To enable multicast VPN, you must configure a VPN routing and forwarding (VRF) instance.

Information About Implementing Multicast Routing

Key Protocols and Features Supported in the Cisco IOS XR Software Multicast Routing Implementation

*Table 5: Supported Features for IPv4 and IPv6*

<table>
<thead>
<tr>
<th>Feature</th>
<th>IPv4 Support</th>
<th>IPv6 Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic host registration</td>
<td>Yes (IGMP v1/2/3)</td>
<td>Yes</td>
</tr>
<tr>
<td>Explicit tracking of hosts, groups, and channels</td>
<td>Yes (IGMP v3)</td>
<td>Yes</td>
</tr>
<tr>
<td>PIM-SM&lt;sup&gt;2&lt;/sup&gt;</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PIM-SSM</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PIM-SSM Mapping</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Auto-RP</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Multicast Routing Functional Overview

Traditional IP communication allows a host to send packets to a single host (unicast transmission) or to all hosts (broadcast transmission). Multicast provides a third scheme, allowing a host to send a single data stream to a subset of all hosts (group transmission) at about the same time. IP hosts are known as group members.

Packets delivered to group members are identified by a single multicast group address. Multicast packets are delivered to a group using best-effort reliability, just like IP unicast packets.

The multicast environment consists of senders and receivers. Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message.

A multicast address is chosen for the receivers in a multicast group. Senders use that group address as the destination address of a datagram to reach all members of the group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. A host can be a member of more than one multicast group at a time.

How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it may be very short-lived. Membership in a group can change constantly. A group that has members may have no activity.

Routers use the Internet Group Management Protocol (IGMP) (IPv4) and Multicast Listener Discovery (MLD) (IPv6) to learn whether members of a group are present on their directly attached subnets. Hosts join multicast groups by sending IGMP or MLD report messages.

Many multimedia applications involve multiple participants. Multicast is naturally suitable for this communication paradigm.
Multicast Routing Implementation

Cisco IOS XR Software supports the following protocols to implement multicast routing:

- IGMP is used between hosts on a LAN and the routers on that LAN to track the multicast groups of which hosts are members.

- Protocol Independent Multicast in sparse mode (PIM-SM) is used between routers so that they can track which multicast packets to forward to each other and to their directly connected LANs.

- Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM) is similar to PIM-SM with the additional ability to report interest in receiving packets from specific source addresses (or from all but the specific source addresses), to an IP multicast address.

- PIM-SSM is made possible by IGMPv3 and MLDv2. Hosts can now indicate interest in specific sources using IGMPv3 and MLDv2. SSM does not require a rendezvous point (RP) to operate.

- PIM Bidirectional is a variant of the Protocol Independent Multicast suit of routing protocols for IP multicast. PIM-BIDIR is designed to be used for many-to-many applications within individual PIM domains.

This image shows IGMP and PIM-SM operating in a multicast environment.

Figure 1: Multicast Routing Protocols
PIM-SM, PIM-SSM, and PIM-BIDIR

Protocol Independent Multicast (PIM) is a multicast routing protocol used to create multicast distribution trees, which are used to forward multicast data packets. PIM is an efficient IP routing protocol that is “independent” of a routing table, unlike other multicast protocols such as Multicast Open Shortest Path First (MOSPF) or Distance Vector Multicast Routing Protocol (DVMRP).

Cisco IOS XR Software supports Protocol Independent Multicast in sparse mode (PIM-SM), Protocol Independent Multicast in Source-Specific Multicast (PIM-SSM), and Protocol Independent Multicast in Bi-directional mode (BIDIR) permitting these modes to operate on your router at the same time.

PIM-SM and PIM-SSM supports one-to-many applications by greatly simplifying the protocol mechanics for deployment ease. Bidir PIM helps deploy emerging communication and financial applications that rely on a many-to-many applications model. BIDIR PIM enables these applications by allowing them to easily scale to a very large number of groups and sources by eliminating the maintenance of source state.

PIM-SM Operations

PIM in sparse mode operation is used in a multicast network when relatively few routers are involved in each multicast and these routers do not forward multicast packets for a group, unless there is an explicit request for the traffic.

For more information about PIM-SM, see the PIM-Sparse Mode, on page 61.

PIM-SSM Operations

PIM in Source-Specific Multicast operation uses information found on source addresses for a multicast group provided by receivers and performs source filtering on traffic.

• By default, PIM-SSM operates in the 232.0.0.0/8 multicast group range for IPv4 and ff3x::/32 (where x is any valid scope) in IPv6. To configure these values, use the ssm range command.
• If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers must be upgraded with Cisco IOS XR Software that supports the SSM feature.
• No MSDP SA messages within the SSM range are accepted, generated, or forwarded.

PIM-Bidirectional Operations

PIM Bidirectional (BIDIR) has one shared tree from sources to RP and from RP to receivers. This is unlike the PIM-SM, which is unidirectional by nature with multiple source trees - one per (S,G) or a shared tree from receiver to RP and multiple SG trees from RP to sources.

Benefits of PIM BIDIR are as follows:

• As many sources for the same group use one and only state (*, G), only minimal states are required in each router.
• No data triggered events.
• Rendezvous Point (RP) router not required. The RP address only needs to be a routable address and need not exist on a physical device.
Restrictions for PIM-SM and PIM-SSM, and PIM BIDIR

Interoperability with SSM
PIM-SM operations within the SSM range of addresses change to PIM-SSM. In this mode, only PIM (S,G) join and prune messages are generated by the router, and no (S,G) RP shared tree or (*,G) shared tree messages are generated.

IGMP Version
To report multicast memberships to neighboring multicast routers, hosts use IGMP, and all routers on the subnet must be configured with the same version of IGMP.

A router running Cisco IOS XR Software does not automatically detect Version 1 systems. You must use the `version` command in router IGMP configuration submode to configure the IGMP version.

PIM-Bidir Restrictions
PIM-Bidir is not supported on MVPN.

Internet Group Management Protocol
Cisco IOS XR Software provides support for Internet Group Management Protocol (IGMP) over IPv4.

IGMP provides a means for hosts to indicate which multicast traffic they are interested in and for routers to control and limit the flow of multicast traffic throughout the network. Routers build state by means of IGMP and MLD messages; that is, router queries and host reports.

A set of queries and hosts that receive multicast data streams from the same source is called a multicast group. Hosts use IGMP and MLD messages to join and leave multicast groups.

Note
IGMP messages use group addresses, which are Class D IP addresses. The high-order four bits of a Class D address are 1110. Host group addresses can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is guaranteed not to be assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

IGMP Versions
The following points describe IGMP versions 1, 2, and 3:

- IGMP Version 1 provides for the basic query-response mechanism that allows the multicast router to determine which multicast groups are active and for other processes that enable hosts to join and leave a multicast group.

- IGMP Version 2 extends IGMP allowing such features as the IGMP query timeout and the maximum query-response time. See RFC 2236.

- IGMP Version 3 permits joins and leaves for certain source and group pairs instead of requesting traffic from all sources in the multicast group.
**IGMP Routing Example**

Figure 2: IGMPv3 Signaling, on page 60 illustrates two sources, 10.0.0.1 and 10.0.1.1, that are multicasting to group 239.1.1.1. The receiver wants to receive traffic addressed to group 239.1.1.1 from source 10.0.0.1 but not from source 10.0.1.1. The host must send an IGMPv3 message containing a list of sources and groups (S, G) that it wants to join and a list of sources and groups (S, G) that it wants to leave. Router C can now use this information to prune traffic from Source 10.0.1.1 so that only Source 10.0.0.1 traffic is being delivered to Router C.

Figure 2: IGMPv3 Signaling

---

**Note**

When configuring IGMP, ensure that all systems on the subnet support the same IGMP version. The router does not automatically detect Version 1 systems. Configure the router for Version 2 if your hosts do not support Version 3.

---

**Protocol Independent Multicast**

Protocol Independent Multicast (PIM) is a routing protocol designed to send and receive multicast routing updates. Proper operation of multicast depends on knowing the unicast paths towards a source or an RP. PIM relies on unicast routing protocols to derive this reverse-path forwarding (RPF) information. As the name PIM implies, it functions independently of the unicast protocols being used. PIM relies on the Routing Information Base (RIB) for RPF information.
If the multicast subsequent address family identifier (SAFI) is configured for Border Gateway Protocol (BGP), or if multicast intact is configured, a separate multicast unicast RIB is created and populated with the BGP multicast SAFI routes, the intact information, and any IGP information in the unicast RIB. Otherwise, PIM gets information directly from the unicast SAFI RIB. Both multicast unicast and unicast databases are outside of the scope of PIM.


Cisco IOS XR Software supports PIM-SM, PIM-SSM, and PIM Version 2 only. PIM Version 1 hello messages that arrive from neighbors are rejected.

---

**PIM-Sparse Mode**

Typically, PIM in sparse mode (PIM-SM) operation is used in a multicast network when relatively few routers are involved in each multicast. Routers do not forward multicast packets for a group, unless there is an explicit request for traffic. Requests are accomplished using PIM join messages, which are sent hop by hop toward the root node of the tree. The root node of a tree in PIM-SM is the rendezvous point (RP) in the case of a shared tree or the first-hop router that is directly connected to the multicast source in the case of a shortest path tree (SPT). The RP keeps track of multicast groups, and the sources that send multicast packets are registered with the RP by the first-hop router of the source.

As a PIM join travels up the tree, routers along the path set up the multicast forwarding state so that the requested multicast traffic is forwarded back down the tree. When multicast traffic is no longer needed, a router sends a PIM prune message up the tree toward the root node to prune (or remove) the unnecessary traffic. As this PIM prune travels hop by hop up the tree, each router updates its forwarding state appropriately. Ultimately, the forwarding state associated with a multicast group or source is removed. Additionally, if prunes are not explicitly sent, the PIM state will timeout and be removed in the absence of any further join messages.

PIM-SM is the best choice for multicast networks that have potential members at the end of WAN links.

**PIM-Source Specific Multicast**

In many multicast deployments where the source is known, protocol-independent multicast-source-specific multicast (PIM-SSM) mapping is the obvious multicast routing protocol choice to use because of its simplicity. Typical multicast deployments that benefit from PIM-SSM consist of entertainment-type solutions like the ETTH space, or financial deployments that completely rely on static forwarding.

PIM-SSM is derived from PIM-SM. However, whereas PIM-SM allows for the data transmission of all sources sending to a particular group in response to PIM join messages, the SSM feature forwards traffic to receivers only from those sources that the receivers have explicitly joined. Because PIM joins and prunes are sent directly towards the source sending traffic, an RP and shared trees are unnecessary and are disallowed. SSM is used to optimize bandwidth utilization and deny unwanted Internet broadcast traffic. The source is provided by interested receivers through IGMPv3 membership reports.

In SSM, delivery of datagrams is based on (S,G) channels. Traffic for one (S,G) channel consists of datagrams with an IP unicast source address S and the multicast group address G as the IP destination address. Systems receive traffic by becoming members of the (S,G) channel. Signaling is not required, but receivers must subscribe or unsubscribe to (S,G) channels to receive or not receive traffic from specific sources. Channel
subscription signaling uses IGMP to include mode membership reports, which are supported only in Version 3 of IGMP (IGMPv3).

To run SSM with IGMPv3, SSM must be supported on the multicast router, the host where the application is running, and the application itself. Cisco IOS XR Software allows SSM configuration for an arbitrary subset of the IP multicast address range 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use addresses in the SSM range, unless the application is modified to use explicit (S,G) channel subscription.

**PIM-Bidirectional Mode**

PIM BIDIR is a variant of the Protocol Independent Multicast (PIM) suite of routing protocols for IP multicast. In PIM, packet traffic for a multicast group is routed according to the rules of the mode configured for that multicast group. In bidirectional mode, traffic is only routed along a bidirectional shared tree that is rooted at the rendezvous point (RP) for the group. In PIM-BIDIR, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address does not need to be a router, but can be any unassigned IP address on a network that is reachable throughout the PIM domain. Using this technique is the preferred configuration for establishing a redundant RP configuration for PIM-BIDIR.

*Note* In Cisco IOS XR Release 4.2.1, Anycast RP is not supported on PIM Bidirectional mode.

PIM-BIDIR is designed to be used for many-to-many applications within individual PIM domains. Multicast groups in bidirectional mode can scale to an arbitrary number of sources without incurring overhead due to the number of sources. PIM-BIDIR is derived from the mechanisms of PIM-sparse mode (PIM-SM) and shares many SPT operations. PIM-BIDIR also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but no registering process for sources as in PIM-SM. These modifications are necessary and sufficient to allow forwarding of traffic in all routers solely based on the (*, G) multicast routing entries. This feature eliminates any source-specific state and allows scaling capability to an arbitrary number of sources.

The traditional PIM protocols (dense-mode and sparse-mode) provided two models for forwarding multicast packets, source trees and shared trees. Source trees are rooted at the source of the traffic while shared trees are rooted at the rendezvous point. Source trees achieve the optimum path between each receiver and the source at the expense of additional routing information: an (S,G) routing entry per source in the multicast routing table. The shared tree provides a single distribution tree for all of the active sources. This means that traffic from different sources traverse the same distribution tree to reach the interested receivers, therefore reducing the amount of routing state in the network. This shared tree needs to be rooted somewhere, and the location of this root is the rendezvous point. PIM BIDIR uses shared trees as their main forwarding mechanism.

The algorithm to elect the designated forwarder is straightforward, all the PIM neighbors in a subnet advertise their unicast route to the rendezvous point and the router with the best route is elected. This effectively builds a shortest path between every subnet and the rendezvous point without consuming any multicast routing state (no (S,G) entries are generated). The designated forwarder election mechanism expects all of the PIM neighbors to be BIDIR enabled. In the case where one of more of the neighbors is not a BIDIR capable router, the election fails and BIDIR is disabled in that subnet.
PIM Shared Tree and Source Tree (Shortest Path Tree)

In PIM-SM, the rendezvous point (RP) is used to bridge sources sending data to a particular group with receivers sending joins for that group. In the initial setup of state, interested receivers receive data from senders to the group across a single data distribution tree rooted at the RP. This type of distribution tree is called a shared tree or rendezvous point tree (RPT) as illustrated in Figure 3: Shared Tree and Source Tree (Shortest Path Tree), on page 63. Data from senders is delivered to the RP for distribution to group members joined to the shared tree.

Figure 3: Shared Tree and Source Tree (Shortest Path Tree)

Unless the `spt-threshold infinity` command is configured, this initial state gives way as soon as traffic is received on the leaf routers (designated router closest to the host receivers). When the leaf router receives traffic from the RP on the RPT, the router initiates a switch to a data distribution tree rooted at the source sending traffic. This type of distribution tree is called a shortest path tree or source tree. By default, the Cisco IOS XR Software switches to a source tree when it receives the first data packet from a source.

The following process describes the move from shared tree to source tree in more detail:

1. Receiver joins a group; leaf Router C sends a join message toward RP.
2. RP puts link to Router C in its outgoing interface list.
3. Source sends data; Router A encapsulates data in Register and sends it to RP.
4. RP forwards data down the shared tree to Router C and sends a join message toward Source. At this point, data may arrive twice at the RP, once encapsulated and once natively.
5. When data arrives natively (unencapsulated) at RP, RP sends a register-stop message to Router A.
6 By default, receipt of the first data packet prompts Router C to send a join message toward Source.

7 When Router C receives data on (S,G), it sends a prune message for Source up the shared tree.

8 RP deletes the link to Router C from outgoing interface of (S,G). RP triggers a prune message toward Source.

Join and prune messages are sent for sources and RPs. They are sent hop by hop and are processed by each PIM router along the path to the source or RP. Register and register-stop messages are not sent hop by hop. They are exchanged using direct unicast communication between the designated router that is directly connected to a source and the RP for the group.

**Tip**
The *spt-threshold infinity* command lets you configure the router so that it never switches to the shortest path tree (SPT).

### Multicast-Intact

The multicast-intact feature provides the ability to run multicast routing (PIM) when Interior Gateway Protocol (IGP) shortcuts are configured and active on the router. Both Open Shortest Path First, version 2 (OSPFv2), and Intermediate System-to-Intermediate System (IS-IS) support the multicast-intact feature. Multiprotocol Label Switching Traffic Engineering (MPLS-TE) and IP multicast coexistence is supported in Cisco IOS XR Software by using the `mpls traffic-eng multicast-intact` IS-IS or OSPF router command. See *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide* for information on configuring multicast intact using IS-IS and OSPF commands.

You can enable multicast-intact in the IGP when multicast routing protocols (PIM) are configured and IGP shortcuts are configured on the router. IGP shortcuts are MPLS tunnels that are exposed to IGP. The IGPs route the IP traffic over these tunnels to destinations that are downstream from the egress router of the tunnel (from an SPF perspective). PIM cannot use IGP shortcuts for propagating PIM joins because reverse path forwarding (RPF) cannot work across a unidirectional tunnel.

When you enable multicast-intact on an IGP, the IGP publishes a parallel or alternate set of equal-cost next-hops for use by PIM. These next-hops are called `mcast-intact next-hops`. The mcast-intact next-hops have the following attributes:

- They are guaranteed not to contain any IGP shortcuts.
- They are not used for unicast routing but are used only by PIM to look up an IPv4 next hop to a PIM source.
- They are not published to the Forwarding Information Base (FIB).
- When multicast-intact is enabled on an IGP, all IPv4 destinations that were learned through link-state advertisements are published with a set equal-cost mcast-intact next-hops to the RIB. This attribute applies even when the native next-hops have no IGP shortcuts.
- In IS-IS, the max-paths limit is applied by counting both the native and mcast-intact next-hops together. (In OSPFv2, the behavior is slightly different.)
Designated Routers

Cisco routers use PIM-SM to forward multicast traffic and follow an election process to select a designated router (DR) when there is more than one router on a LAN segment.

The designated router is responsible for sending PIM register and PIM join and prune messages toward the RP to inform it about host group membership.

If there are multiple PIM-SM routers on a LAN, a designated router must be elected to avoid duplicating multicast traffic for connected hosts. The PIM router with the highest IP address becomes the DR for the LAN unless you choose to force the DR election by use of the `dr-priority` command. The DR priority option allows you to specify the DR priority of each router on the LAN segment (default priority = 1) so that the router with the highest priority is elected as the DR. If all routers on the LAN segment have the same priority, the highest IP address is again used as the tiebreaker.

Figure 4: Designated Router Election on a Multiaccess Segment, on page 66 illustrates what happens on a multiaccess segment. Router A (10.0.0.253) and Router B (10.0.0.251) are connected to a common multiaccess Ethernet segment with Host A (10.0.0.1) as an active receiver for Group A. As the Explicit Join model is used, only Router A, operating as the DR, sends joins to the RP to construct the shared tree for Group A. If Router B were also permitted to send (*, G) joins to the RP, parallel paths would be created and Host A would receive duplicate multicast traffic. When Host A begins to source multicast traffic to the group, the DR’s responsibility is to send register messages to the RP. Again, if both routers were assigned the responsibility, the RP would receive duplicate multicast packets.

If the DR fails, the PIM-SM provides a way to detect the failure of Router A and to elect a failover DR. If the DR (Router A) were to become inoperable, Router B would detect this situation when its neighbor adjacency with Router A timed out. Because Router B has been hearing IGMP membership reports from Host A, it already has IGMP state for Group A on this interface and immediately sends a join to the RP when it becomes the new DR. This step reestablishes traffic flow down a new branch of the shared tree using Router B. Additionally, if Host A were sourcing traffic, Router B would initiate a new register process immediately after receiving the next multicast packet from Host A. This action would trigger the RP to join the SPT to Host A, using a new branch through Router B.
Two PIM routers are neighbors if there is a direct connection between them. To display your PIM neighbors, use the `show pim neighbor` command in EXEC mode.

**Figure 4: Designated Router Election on a Multiaccess Segment**

**Tip**

Rendezvous Points

When PIM is configured in sparse mode, you must choose one or more routers to operate as a rendezvous point (RP). A rendezvous point is a single common root placed at a chosen point of a shared distribution tree, as illustrated in Figure 3: Shared Tree and Source Tree (Shortest Path Tree), on page 63. A rendezvous point can be either configured statically in each box or learned through a dynamic mechanism.

PIM DRs forward data from directly connected multicast sources to the rendezvous point for distribution down the shared tree. Data is forwarded to the rendezvous point in one of two ways:

- Encapsulated in register packets and unicast directly to the rendezvous point by the first-hop router operating as the DR
- Multicast forwarded by the RPF forwarding algorithm, described in the Reverse-Path Forwarding, on page 68, if the rendezvous point has itself joined the source tree.
The rendezvous point address is used by first-hop routers to send PIM register messages on behalf of a host sending a packet to the group. The rendezvous point address is also used by last-hop routers to send PIM join and prune messages to the rendezvous point to inform it about group membership. You must configure the rendezvous point address on all routers (including the rendezvous point router).

A PIM router can be a rendezvous point for more than one group. Only one rendezvous point address can be used at a time within a PIM domain. The conditions specified by the access list determine for which groups the router is a rendezvous point.

You can either manually configure a PIM router to function as a rendezvous point or allow the rendezvous point to learn group-to-RP mappings automatically by configuring Auto-RP or BSR. (For more information, see the Auto-RP, on page 67 section that follows and PIM Bootstrap Router, on page 68.)

Auto-RP

Automatic route processing (Auto-RP) is a feature that automates the distribution of group-to-RP mappings in a PIM network. This feature has these benefits:

- It is easy to use multiple RPs within a network to serve different group ranges.
- It allows load splitting among different RPs.
- It facilitates the arrangement of RPs according to the location of group participants.
- It avoids inconsistent, manual RP configurations that might cause connectivity problems.

Multiple RPs can be used to serve different group ranges or to serve as hot backups for each other. To ensure that Auto-RP functions, configure routers as candidate RPs so that they can announce their interest in operating as an RP for certain group ranges. Additionally, a router must be designated as an RP-mapping agent that receives the RP-announcement messages from the candidate RPs, and arbitrates conflicts. The RP-mapping agent sends the consistent group-to-RP mappings to all remaining routers. Thus, all routers automatically determine which RP to use for the groups they support.

Tip

By default, if a given group address is covered by group-to-RP mappings from both static RP configuration, and is discovered using Auto-RP or PIM BSR, the Auto-RP or PIM BSR range is preferred. To override the default, and use only the RP mapping, use the `rp-address override` keyword.

Note

If you configure PIM in sparse mode and do not configure Auto-RP, you must statically configure an RP as described in the Configuring a Static RP and Allowing Backward Compatibility, on page 106. When router interfaces are configured in sparse mode, Auto-RP can still be used if all routers are configured with a static RP address for the Auto-RP groups.

Note

Auto-RP is not supported on VRF interfaces. Auto-RP Lite allows you to configure auto-RP on the CE router. It allows the PE router that has the VRF interface to relay auto-RP discovery, and announce messages across the core and eventually to the remote CE. Auto-RP is supported in only the IPv4 address family.
**PIM Bootstrap Router**

The PIM bootstrap router (BSR) provides a fault-tolerant, automated RP discovery and distribution mechanism that simplifies the Auto-RP process. This feature is enabled by default allowing routers to dynamically learn the group-to-RP mappings.

PIM uses the BSR to discover and announce RP-set information for each group prefix to all the routers in a PIM domain. This is the same function accomplished by Auto-RP, but the BSR is part of the PIM Version 2 specification. The BSR mechanism interoperates with Auto-RP on Cisco routers.

To avoid a single point of failure, you can configure several candidate BSRs in a PIM domain. A BSR is elected among the candidate BSRs automatically. Candidates use bootstrap messages to discover which BSR has the highest priority. The candidate with the highest priority sends an announcement to all PIM routers in the PIM domain that it is the BSR.

Routers that are configured as candidate RPs unicast to the BSR the group range for which they are responsible. The BSR includes this information in its bootstrap messages and disseminates it to all PIM routers in the domain. Based on this information, all routers are able to map multicast groups to specific RPs. As long as a router is receiving the bootstrap message, it has a current RP map.

**Reverse-Path Forwarding**

Reverse-path forwarding (RPF) is an algorithm used for forwarding multicast datagrams. It functions as follows:

- If a router receives a datagram on an interface it uses to send unicast packets to the source, the packet has arrived on the RPF interface.
- If the packet arrives on the RPF interface, a router forwards the packet out the interfaces present in the outgoing interface list of a multicast routing table entry.
- If the packet does not arrive on the RPF interface, the packet is silently discarded to prevent loops.

PIM uses both source trees and RP-rooted shared trees to forward datagrams; the RPF check is performed differently for each, as follows:

- If a PIM router has an (S,G) entry present in the multicast routing table (a source-tree state), the router performs the RPF check against the IP address of the source for the multicast packet.
- If a PIM router has no explicit source-tree state, this is considered a shared-tree state. The router performs the RPF check on the address of the RP, which is known when members join the group.

Sparse-mode PIM uses the RPF lookup function to determine where it needs to send joins and prunes. (S,G) joins (which are source-tree states) are sent toward the source. (*,G) joins (which are shared-tree states) are sent toward the RP.

**Multicast VPN**

Multicast VPN (MVPN) provides the ability to dynamically provide multicast support over MPLS networks. MVPN introduces an additional set of protocols and procedures that help enable a provider to support multicast traffic in a VPN.
PIM-Bidir is not supported on MVPN.

There are two ways MCAST VPN traffic can be transported over the core network:

- **Rosen GRE (native):** MVPN uses GRE with unique multicast distribution tree (MDT) forwarding to enable scalability of native IP Multicast in the core network. MVPN introduces multicast routing information to the VPN routing and forwarding table (VRF), creating a Multicast VRF. In Rosen GRE, the MCAST customer packets (c-packets) are encapsulated into the provider MCAST packets (p-packets), so that the PIM protocol is enabled in the provider core, and mrib/mfib is used for forwarding p-packets in the core.

- **MLDP ones (Rosen, partition):** MVPN allows a service provider to configure and support multicast traffic in an MPLS VPN environment. This type supports routing and forwarding of multicast packets for each individual VPN routing and forwarding (VRF) instance, and it also provides a mechanism to transport VPN multicast packets across the service provider backbone. In the MLDP case, the regular label switch path forwarding is used, so core does not need to run PIM protocol. In this scenario, the c-packets are encapsulated in the MPLS labels and forwarding is based on the MPLS Label Switched Paths (LSPs), similar to the unicast case.

In both the above types, the MVPN service allows you to build a Protocol Independent Multicast (PIM) domain that has sources and receivers located in different sites.

To provide Layer 3 multicast services to customers with multiple distributed sites, service providers look for a secure and scalable mechanism to transmit customer multicast traffic across the provider network. Multicast VPN (MVPN) provides such services over a shared service provider backbone, using native multicast technology similar to BGP/MPLS VPN.

In addition to all the ethernet based line cards, MVPN is also supported on the Cisco ASR 9000 Series SPA Interface Processor-700 card from the Cisco IOS XR Software Release 4.0 onwards. Cisco ASR 9000 Series SPA Interface Processor-700 enables the Cisco ASR 9000 Series Routers to support multiple legacy services (such as TDM and ATM) on a router that is primarily designed for Ethernet networks. Cisco ASR 9000 Series SPA Interface Processor-700 is QFP-based and therefore has the flexibility and service scale offered by Cisco ASIC and the reliability of Cisco IOS XR Software.

MVPN emulates MPLS VPN technology in its adoption of the multicast domain (MD) concept, in which provider edge (PE) routers establish virtual PIM neighbor connections with other PE routers that are connected to the same customer VPN. These PE routers thereby form a secure, virtual multicast domain over the provider network. Multicast traffic is then transmitted across the core network from one site to another, as if the traffic were going through a dedicated provider network.

Multi-instance BGP is supported on multicast and MVPN. Multicast-related SAFIs can be configured on multiple BGP instances.

### Multicast VPN Routing and Forwarding

Dedicated multicast routing and forwarding tables are created for each VPN to separate traffic in one VPN from traffic in another.

The VPN-specific multicast routing and forwarding database is referred to as **MVRF**. On a PE router, an MVRF is created when multicast is enabled for a VRF. Protocol Independent Multicast (PIM), and Internet Group Management Protocol (IGMP) protocols run in the context of MVRF, and all routes created by an MVRF protocol instance are associated with the corresponding MVRF. In addition to VRFs, which hold...
VPN-specific protocol states, a PE router always has a global VRF instance, containing all routing and forwarding information for the provider network.

**Multicast Distribution Tree Tunnels**

The multicast distribution tree (MDT) can span multiple customer sites through provider networks, allowing traffic to flow from one source to multiple receivers. For MLDP, the MDT tunnel trees are called as Labeled MDT (LMDT).

Secure data transmission of multicast packets sent from the customer edge (CE) router at the ingress PE router is achieved by encapsulating the packets in a provider header and transmitting the packets across the core. At the egress PE router, the encapsulated packets are decapsulated and then sent to the CE receiving routers.

Multicast distribution tree (MDT) tunnels are point-to-multipoint. A MDT tunnel interface is an interface that MVRF uses to access the multicast domain. It can be deemed as a passage that connects an MVRF and the global MVRF. Packets sent to an MDT tunnel interface are received by multiple receiving routers. Packets sent to an MDT tunnel interface are encapsulated, and packets received from a MDT tunnel interface are decapsulated.

**Figure 5: Virtual PIM Peer Connection over an MDT Tunnel Interface**

Encapsulating multicast packets in a provider header allows PE routers to be kept unaware of the packets’ origin—all VPN packets passing through the provider network are viewed as native multicast packets and are routed based on the routing information in the core network. To support MVPN, PE routers only need to support native multicast routing.

MVPN also supports optimized VPN traffic forwarding for high-bandwidth applications that have sparsely distributed receivers. A dedicated multicast group can be used to encapsulate packets from a specific source, and an optimized MDT can be created to send traffic only to PE routers connected to interested receivers. This is referred to as data MDT.

**InterAS Support on Multicast VPN**

The Multicast VPN Inter-AS Support feature enables service providers to provide multicast connectivity to VPN sites that span across multiple autonomous systems. This feature was added to MLDP profile that enables Multicast Distribution Trees (MDTs), used for Multicast VPNs (MVPNs), to span multiple autonomous systems.

There are two types of MVPN inter-AS deployment scenarios:
- Single-Provider Inter-AS—A service provider whose internal network consists of multiple autonomous systems.

- Intra-Provider Inter-AS—Multiple service providers that need to coordinate their networks to provide inter-AS support.

To establish a Multicast VPN between two autonomous systems, a MDT-default tunnel must be set up between the two PE routers. The PE routers accomplish this by joining the configured MDT-default group. This MDT-default group is configured on the PE router and is unique for each VPN. The PIM sends the join based on the mode of the groups, which can be PIM SSM, or sparse mode.

**Note**

PIM-Bidir is not supported on MVPN.

---

**Benefits of MVPN Inter-AS Support**

The MVPN Inter-AS Support feature provides these benefits to service providers:

- Increased multicast coverage to customers that require multicast to span multiple services providers in an MPLS Layer 3 VPN service.

- The ability to consolidate an existing MVPN service with another MVPN service, as in the case of a company merger or acquisition.

**InterAS Option A**

InterAS Option A is the basic Multicast VPN configuration option. In this option, the PE router partially plays the Autonomous System Border Router (ASBR) role in each Autonomous System (AS). Such a PE router in each AS is directly connected through multiple VRF bearing subinterfaces. MPLS label distribution protocol need not run between these InterAS peering PE routers. However, an IGP or BGP protocol can be used for route distribution under the VRF.

The Option A model assumes direct connectivity between PE routers of different autonomous systems. The PE routers are attached by multiple physical or logical interfaces, each of which is associated with a given VPN (through a VRF instance). Each PE router, therefore, treats the adjacent PE router like a customer edge (CE) router. The standard Layer 3 MPLS VPN mechanisms are used for route redistribution with each autonomous system; that is, the PEs use exterior BGP (eBGP) to distribute unlabeled IPv4 addresses to each other.

**Note**

Option A allows service providers to isolate each autonomous system from the other. This provides better control over routing exchanges and security between the two networks. However, Option A is considered the least scalable of all the inter-AS connectivity options.

**InterAS Option B**

InterAS Option B is a model that enables VPNv4 route exchanges between the ASBRs. This model also distributes BGP MVPN address family. In this model, the PE routers use internal BGP (iBGP) to redistribute labeled VPNv4 routes either to an ASBR or to route reflector of which an ASBR is a client. These ASBRs use multiprotocol eBGP (MP-eBGP) to advertise VPNv4 routes into the local autonomous systems. The MP-eBGP advertises VPNv4 prefix and label information across the service provider boundaries. The
advertising ASBR router replaces the two-level label stack, which it uses to reach the originating PE router and VPN destination in the local autonomous system, with a locally allocated label before advertising the VPNv4 route. This replacement happens because the next-hop attribute of all routes advertised between the two service providers is reset to the ASBR router's peering address, thus making the ASBR router the termination point of the label-switched path (LSP) for the advertised routes. To preserve the LSP between ingress and egress PE routers, the ASBR router allocates a local label that is used to identify the label stack of the route within the local VPN network. This newly allocated label is set on packets sent towards the prefix from the adjacent service provider.

**Note**
Option B enables service providers to isolate both autonomous systems with the added advantage that it scales to a higher degree than Option A.

In the InterAS Option B model, only BGP-AD profiles are supported:

- MLDP MS-PMSI MP2MP with BGP-AD (profile 4)
- Rosen GRE with or without BGP-AD (profile 9)

**Note** Profile 9 is only supported with leaking root address into IGP.

MLDP MS-PMSI MP2MP with BGP-AD (profile 5) is not supported.

**InterAS Option C**

InterAS Option C allows exchange of VPNv4 routes between router reflectors (RRs) using multihop eBGP peering sessions. In this model, the MP-eBGP exchange of VPNv4 routes between the RRs of different autonomous systems is combined with the next hops for these routes exchanges between corresponding ASBR routers. This model also distributes BGP MVPN address family along with VPNv4. This model neither allows the VPNv4 routes to be maintained nor distributes by the ASBRs. ASBRs maintains labeled IPv4 routes to the PE routers within its autonomous system and uses eBGP to distribute these routes to other autonomous systems. In any transit autonomous systems, the ASBRs uses eBGP to pass along the labeled IPv4 routes, resulting in the creation of a LSP from the ingress PE router to the egress PE router.

Option C model uses the multihop functionality to allow the establishment for MP-eBGP peering sessions as the RRs of different autonomous systems are not directly connected. The RRs also do not reset the next-hop attribute of the VPNv4 routes when advertising them to adjacent autonomous systems as these do not attract the traffic for the destinations that they advertise, making it mandatory to enable the exchange of next hops. These are just a relay station between the source and receiver PEs. The PE router next-hop addresses for the VPNv4 routes, thus, are exchanged between ASBR routers. The exchange of these addresses between autonomous systems is accomplished by redistributing the PE router /32 addresses between the autonomous systems or by using BGP label distribution.

**Note** Option C normally is deployed only when each autonomous system belongs to the same overall authority, such as a global Layer 3 MPLS VPN service provider with global autonomous systems.

In the InterAS Option C model, these profiles are supported:
IPv6 Connectivity over MVPN

On the Cisco ASR 9000 Series Routers, in Cisco IOS XR Software starting Release 4.2.1, IPv6 connectivity is supported between customer sites over an IPv4-only core network with a default VRF. VPN PE routers interoperate between the two address families, with control and forwarding actions between IPv4-encapsulated MDTs and IPv6 customer routes. IPv6 users can configure IPv6-over-IPv4 multicast VPN support through BGP.

In Cisco IOS XR Software, MVPNv6 can have a separate data mdt group configured, which can be different from MVPNv4. But both MVPNv6 and MVPNv4 must have the same default mdt group configured.

The configuration example below shows MVPNv6 data mdt:

```plaintext
vrf cisco-sjc1
  address-family ipv4
    mdt data 226.8.3.0/24 threshold 5
  mdt default ipv4 226.8.0.1
!
address-family ipv6
  mdt data 226.8.4.0/24 threshold 5
  mdt default ipv4 226.8.0.1
!
```

BGP Requirements

PE routers are the only routers that need to be MVPN-aware and able to signal remote PEs with information regarding the MVPN. It is fundamental that all PE routers have a BGP relationship with each other, either directly or through a route reflector, because the PE routers use the BGP peering address information to derive the RPF PE peer within a given VRF.

PIM-SSM MDT tunnels cannot be set up without a configured BGP MDT address-family, because you establish the tunnels, using the BGP connector attribute.

See the Implementing BGP on Cisco IOS XR Software module of the Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide for information on BGP support for Multicast VPN.

MVPN Static P2MP TE

This feature describes the Multicast VPN (MVPN) support for Multicast over Point-to-Multipoint -Traffic Engineering (P2MP-TE). Currently, Cisco IOS-XR Software supports P2MP-TE only in the Global table and the (S,G) route in the global table can be mapped to P2MP-TE tunnels. However, this feature now enables service providers to use P2MP-TE tunnels to carry VRF multicast traffic. Static mapping is used to map VRF (S, G) traffic to P2MP-TE tunnels, and BGP-AD is used to send P2MP BGP opaque that includes VRF-based P2MP FEC as MDT Selective Provider Multicast Service Interface (S-PMSI).

The advantages of the MVPN support for Multicast over P2MP-TE are:
• Supports traffic engineering such as bandwidth reservation, bandwidth sharing, forwarding replication, explicit routing, and Fast ReRoute (FRR).
• Supports the mapping of multiple multicast streams onto tunnels.

![Figure 6: Multicast VRF](image)

On PE1 router, multicast S,G (video) traffic is received on a VRF interface. The multicast S,G routes are statically mapped to P2MP-TE tunnels. The head-end then originates an S-PMSI (Type-3) BGP-AD route, for each of the S,Gs, with a PMSI Tunnel Attribute (PTA) specifying the P2MP-TE tunnel as the core-tree. The type of the PTA is set to RSVP-TE P2MPLS and the format of the PTA Tunnel-identifier <Extended Tunnel ID, Reserved, Tunnel ID, P2MP ID>, as carried in the RSVP-TE P2MP LSP SESSION Object. Multiple S,G A-D routes can have the same PMSI Tunnel Attribute.

The tail-end PEs (PE2, PE3) receive and cache these S-PMSI updates (sent by all head-end PEs). If there is an S,G Join present in the VRF, with the Upstream Multicast Hop (UMH) across the core, then the PE looks for an S-PMSI announcement from the UMH. If an S-PMSI route is found with a P2MP-TE PTA, then the PE associates the tail label(s) of the Tunnel, with that VRF. When a packet arrives on the P2MP-TE tunnel, the tail-end removes the label and does an S,G lookup in the 'associated' VRF. If a match is found, the packet is forwarded as per its outgoing information.

**Multitopology Routing**

Multitopology routing allows you to manipulate network traffic flow when desirable (for example, to broadcast duplicate video streams) to flow over non-overlapping paths.

At the core of multitopology routing technology is router space infrastructure (RSI). RSI manages the global configuration of routing tables. These tables are hierarchically organized into VRF tables under logical routers. By default, RSI creates tables for unicast and multicast for both IPv4 and IPv6 under the default VRF. Using multitopology routing, you can configure named topologies for the default VRF.

PIM uses a routing policy that supports matching on source or group address to select the topology in which to look up the reverse-path forwarding (RPF) path to the source. If you do not configure a policy, the existing behavior (to select a default table) remains in force.

Currently, IS-IS and PIM routing protocols alone support multitopology-enabled network.
Multicast VPN Extranet Routing

Multicast VPN (MVPN) extranet routing lets service providers distribute IP multicast content from one enterprise site to another across a multicast VRF. In other words, this feature provides capability to seamlessly hop VRF boundaries to distribute multicast content end to end.

Unicast extranet can be achieved simply by configuring matching route targets across VRFs. However, multicast extranet requires such configuration to resolve route lookups across VRFs in addition to the following:

- Maintain multicast topology maps across VRFs.
- Maintain multicast distribution trees to forward traffic across VRFs.

Information About Extranets

An extranet can be viewed as part of an enterprise intranet that is extended to users outside the enterprise. A VPN is used as a way to do business with other enterprises and with customers, such as selling products and maintaining strong business partnerships. An extranet is a VPN that connects to one or more corporate sites to external business partners or suppliers to securely share a designated part of the enterprise’s business information or operations.

MVPN extranet routing can be used to solve such business problems as:

- Inefficient content distribution between enterprises.
- Inefficient content distribution from service providers or content providers to their enterprise VPN customers.

MVPN extranet routing provides support for IPv4 and IPv6 address family.

An extranet network requires the PE routers to pass traffic across VRFs (labeled “P” in Figure 7: Components of an Extranet VPN, on page 76). Extranet networks can run either IPv4 or IPv6, but the core network always runs only IPv4 active multicast.
Extranet Components

**Figure 7: Components of an Extranet MVPN**

MVRF—Multicast VPN routing and forwarding (VRF) instance. An MVRF is a multicast-enabled VRF. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

Source MVRF—An MVRF that can reach the source through a directly connected customer edge (CE) router.

Receiver MVRF—An MVRF to which receivers are connected through one or more CE devices.

Source PE—A PE router that has a multicast source behind a directly connected CE router.

Receiver PE—A PE router that has one or more interested receivers behind a directly connected CE router.

Information About the Extranet MVPN Routing Topology

In unicast routing of peer-to-peer VPNs, BGP routing protocol is used to advertise VPN IPv4 and IPv6 customer routes between provider edge (PE) routers. However, in an MVPN extranet peer-to-peer network, PIM RPF is used to determine whether the RPF next hop is in the same or a different VRF and whether that source VRF is local or remote to the PE.

**Source MVRF on a Receiver PE Router**

To provide extranet MVPN services to enterprise VPN customers by configuring a source MVRF on a receiver PE router, you would complete the following procedure:

- On a receiver PE router that has one or more interested receivers in an extranet site behind a directly connected CE router, configure an MVRF that has the same default MDT group as the site connected to the multicast source.

- On the receiver PE router, configure the same unicast routing policy to import routes from the source MVRF to the receiver MVRF.
If the originating MVRF of the RPF next hop is local (source MVRF at receiver PE router), the join state of the receiver VRFs propagates over the core by using the default multicast distribution tree (MDT) of the source VRF. Figure 8: Source MVRF at the Receiver PE Router, on page 77 illustrates the flow of multicast traffic in an extranet MVVPN topology where the source MVRF is configured on a receiver PE router (source at receiver MVRF topology). An MVRF is configured for VPN-A and VPN-B on PE2, a receiver PE router. A multicast source behind PE1, the source PE router, is sending out a multicast stream to the MVRF for VPN-A, and there are interested receivers behind PE2, the receiver PE router for VPN-B, and also behind PE3, the receiver PE router for VPN-A. After PE1 receives the packets from the source in the MVRF for VPN-A, it replicates and forwards the packets to PE2 and PE3. The packets received at PE2 in VPN-A are decapsulated and replicated to receivers in VPN-B.

Figure 8: Source MVRF at the Receiver PE Router

Receiver MVRF on the Source PE Router

To provide extranet MVVPN services to enterprise VPN customers by configuring the receiver MVRF on the source PE router, complete the following procedure:

- For each extranet site, you would configure an additional MVRF on the source PE router, which has the same default MDT group as the receiver MVRF, if the MVRF is not already configured on the source PE.

- In the receiver MVRF configuration, you would configure the same unicast routing policy on the source and receiver PE routers to import routes from the source MVRF to the receiver MVRF.

If the originating MVRF of the RPF next-hop is remote (receiver MVRF on the source PE router), then the join state of receiver VRFs propagates over the core through the MDT of each receiver.

Figure 9: Receiver MVRF at the Source PE Router Receiver, on page 78 illustrates the flow of multicast traffic in an extranet MVVPN topology where a receiver MVRF is configured on the source PE router. An MVRF is configured for VPN-A and VPN-B on PE1, the source PE router. A multicast source behind PE1 is sending out a multicast stream to the MVRF for VPN-A, and there are interested receivers behind PE2 and PE3, the receiver PE routers for VPN-B and VPN-A, respectively. After PE1 receives the packets from the source in the MVRF for VPN-A, it independently replicates and encapsulates the packets in the MVRF for
VPN-A and VPN-B and forwards the packets. After receiving the packets from this source, PE2 and PE3 decapsulate and forward the packets to the respective MVRFs.

**Figure 9: Receiver MVRF at the Source PE Router Receiver**

For more information, see also Configuring MVVPN Extranet Routing, on page 162 and Configuring MVVPN Extranet Routing: Example, on page 207.

### RPF Policies in an Extranet

RPF policies can be configured in receiver VRFs to bypass RPF lookup in receiver VRFs and statically propagate join states to specified source VRF. Such policies can be configured to pick a source VRF based on either multicast group range, multicast source range, or RP address.

For more information about configuration of RFP policies in extranets, see Configuring RPL Policies in Receiver VRFs to Propagate Joins to a Source VRF: Example, on page 209 and Configuring RPL Policies in Receiver VRFs on Source PE Routers to Propagate Joins to a Source VRF: Example, on page 211.

### Multicast VPN Hub and Spoke Topology

Hub and spoke topology is an interconnection of two categories of sites — Hub sites and Spoke sites. The routes advertised across sites are such that they achieve connectivity in a restricted hub and spoke fashion. A spoke can interact only with its hub because the rest of the network (that is, other hubs and spokes) appears hidden behind the hub.

The hub and spoke topology can be adopted for these reasons:

- Spoke sites of a VPN customer receives all their traffic from a central (or Hub) site hosting services such as server farms.
- Spoke sites of a VPN customer requires all the connectivity between its spoke sites through a central site. This means that the hub site becomes a transit point for interspoke connectivity.
Spoke sites of a VPN customer do not need any connectivity between spoke sites. Hubs can send and receive traffic from all sites but spoke sites can send or receive traffic only to or from Hub sites.

Realizing the Hub and Spoke Topology

Hub and Spoke implementation leverages the infrastructure built for MVPN Extranet. The regular MVPN follows the model in which packets can flow from any site to the other sites. But Hub and Spoke MVPN will restrict traffic flows based on their subscription.

A site can be considered to be a geographic location with a group of CE routers and other devices, such as server farms, connected to PE routers by PE-CE links for VPN access. Either every site can be placed in a separate VRF, or multiple sites can be combined in one VRF on the PE router.

By provisioning every site in a separate VRF, you can simplify the unicast and multicast Hub and Spoke implementation. Such a configuration brings natural protection from traffic leakage - from one spoke site to another. Cisco IOS XR Software implementation of hub and spoke follows the one-site-to-one VRF model. Any site can be designated as either a hub or spoke site, based on how the import or export of routes is setup. Multiple hub and spoke sites can be collated on a given PE router.

Unicast Hub and Spoke connectivity is achieved by the spoke sites importing routes from only Hub sites, and Hub sites importing routes from all sites. As the spoke sites do not exchange routes, spoke to spoke site traffic cannot flow. If interspoke connectivity is required, hubs can choose to re-inject routes learned from one spoke site into other spoke site.

MVPN Hub and Spoke is achieved by separating core tunnels, for traffic sourced from hub sites, and spoke sites. MDT hub is the tunnel carrying traffic sourced from all Hub sites, and MDT spoke carries traffic sourced from all spoke sites. Such tunnel end-points are configured on all PEs participating in hub and spoke topology. If spoke sites do not host any multicast sources or RPs, provisioning of MDT Spoke can be completely avoided at all such routers.

Once these tunnels are provisioned, multicast traffic path will be policy routed in this manner:

1. Hub sites will send traffic to only MDT Hub.
2. Spoke sites will send traffic to only MDT Spoke.
3. Hub sites will receive traffic from both tunnels.
4. Spoke sites will receive traffic from only MDT Hub.

These rules ensure that hubs and spokes can send and receive traffic to or from each other, but direct spoke to spoke communication does not exist. If required, interspoke multicast can flow by turning around the traffic at Hub sites.

These enhancements are made to the Multicast Hub and Spoke topology in Cisco IOS XR Software Release 4.0:

- Auto-RP and BSR are supported across VRFs that are connected through extranet. It is no longer restricted to using static RP only.
- MP-BGP can publish matching import route-targets while passing prefix nexthop information to RIB.
- Route policies can use extended community route targets instead of IP address ranges.
- Support for extranet v4 data mdt was included so that data mdt in hub and spoke can be implemented.
Label Switched Multicast (LSM) Multicast Label Distribution Protocol (mLDP) based Multicast VPN (mVPN) Support

Label Switched Multicast (LSM) is MPLS technology extensions to support multicast using label encapsulation. Next-generation MVPN is based on Multicast Label Distribution Protocol (mLDP), which can be used to build P2MP and MP2MP LSPs through a MPLS network. These LSPs can be used for transporting both IPv4 and IPv6 multicast packets, either in the global table or VPN context.

Benefits of LSM MLDP based MVPN

LSM provides these benefits when compared to GRE core tunnels that are currently used to transport customer traffic in the core:

- It leverages the MPLS infrastructure for transporting IP multicast packets, providing a common data plane for unicast and multicast.
- It applies the benefits of MPLS to IP multicast such as Fast ReRoute (FRR) and
- It eliminates the complexity associated PIM.

Configuring MLDP MVPN

The MLDP MVPN configuration enables IPv4 multicast packet delivery using MPLS. This configuration uses MPLS labels to construct default and data Multicast Distribution Trees (MDTs). The MPLS replication is used as a forwarding mechanism in the core network. For MLDP MVPN configuration to work, ensure that the global MPLS mLDP configuration is enabled. To configure MVPN extranet support, configure the source
multicast VPN Routing and Forwarding (mVRF) on the receiver Provider Edge (PE) router or configure the receiver mVRF on the source PE. MLDP MVPN is supported for both intranet and extranet.

Figure 10: MLDP based MPLS Network

P2MP and MP2MP Label Switched Paths

mLDP is an application that sets up Multipoint Label Switched Paths (MP LSPs) in MPLS networks without requiring multicast routing protocols in the MPLS core. mLDP constructs the P2MP or MP2MP LSPs without interacting with or relying upon any other multicast tree construction protocol. Using LDP extensions for MP LSPs and Unicast IP routing, mLDP can setup MP LSPs. The two types of MP LSPs that can be setup are Point-to-Multipoint (P2MP) and Multipoint-to-Multipoint (MP2MP) type LSPs.

A P2MP LSP allows traffic from a single root (ingress node) to be delivered to a number of leaves (egress nodes), where each P2MP tree is uniquely identified with a 2-tuple (root node address, P2MP LSP identifier). A P2MP LSP consists of a single root node, zero or more transit nodes, and one or more leaf nodes, where typically root and leaf nodes are PEs and transit nodes are P routers. A P2MP LSP setup is receiver-driven and is signaled using mLDP P2MP FEC, where LSP identifier is represented by the MP Opaque Value element. MP Opaque Value carries information that is known to ingress LSRs and Leaf LSRs, but need not be interpreted by transit LSRs. There can be several MP LSPs rooted at a given ingress node, each with its own identifier.

A MP2MP LSP allows traffic from multiple ingress nodes to be delivered to multiple egress nodes, where a MP2MP tree is uniquely identified with a 2-tuple (root node address, MP2MP LSP identifier). For a MP2MP LSP, all egress nodes, except the sending node, receive a packet sent from an ingress node.

A MP2MP LSP is similar to a P2MP LSP, but each leaf node acts as both an ingress and egress node. To build an MP2MP LSP, you can setup a downstream path and an upstream path so that:

- Downstream path is setup just like a normal P2MP LSP
- Upstream path is setup like a P2P LSP towards the upstream router, but inherits the downstream labels from the downstream P2MP LSP.
Packet Flow in mLDP-based Multicast VPN

For each packet coming in, MPLS creates multiple out-labels. Packets from the source network are replicated along the path to the receiver network. The CE1 router sends out the native IP multicast traffic. The PE1 router imposes a label on the incoming multicast packet and replicates the labeled packet towards the MPLS core network. When the packet reaches the core router (P), the packet is replicated with the appropriate labels for the MP2MP default MDT or the P2MP data MDT and transported to all the egress PEs. Once the packet reaches the egress PE, the label is removed and the IP multicast packet is replicated onto the VRF interface.

Realizing a mLDP-based Multicast VPN

There are different ways a Label Switched Path (LSP) built by mLDP can be used depending on the requirement and nature of application such as:

- P2M LSPs for global table transit Multicast using in-band signaling.
- P2MP/MP2MP LSPs for MVPN based on MI-PMSI or Multidirectional Inclusive Provider Multicast Service Instance (Rosen Draft).
- P2MP/MP2MP LSPs for MVPN based on MS-PMSI or Multidirectional Selective Provider Multicast Service Instance (Partitioned E-LAN).

The Cisco ASR 9000 Series Router performs the following important functions for the implementation of MLDP:

1. Encapsulating VRF multicast IP packet with GRE/Label and replicating to core interfaces (imposition node).
2. Replicating multicast label packets to different interfaces with different labels (Mid node).
3. Decapsulate and replicate label packets into VRF interfaces (Disposition node).

Characteristics of mLDP Profiles

The characteristics of various mLDP profiles are listed in this section.

Profile 1: Rosen-mLDP (with no BGP-AD)

These are the characteristics of this profile:

- MP2MP mLDP trees are used in the core.
- VPN-ID is used as the VRF distinguisher.
- Configuration based on Default MDTs.
- Same Default-MDT core-tree used for IPv4 and IPv6 traffic.
- Data-MDT announcements sent by PIM (over Default-MDT).
- The multicast traffic can either be SM or SSM.
- Inter-AS Options A, B, and C are supported. Connector Attribute is announced in VPN-IP routes.
Profile 2: MS-PMSI-mLDP-MP2MP (No BGP-AD)

These are the characteristics of this profile:

- MP2MP mLDP trees are used in the core.
- Different MS-PMSI core-trees for IPv4 and IPv6 traffic.
- The multicast traffic can be SM or SSM.
- Extranet, Hub and Spoke are supported.
- Inter-AS Options A, B, and C are supported. Connector Attribute is announced in VPN-IP routes.

Profile 3: Rosen-GRE with BGP-AD

These are the characteristics of this profile:

- PIM-trees are used in the core. The data encapsulation method used is GRE.
- SM or SSM used in the core.
- Configuration is based on Default-MDTs.
- The multicast traffic can be SM or SSM.
- MoFRR in the core is supported.
- Extranet, Hub and Spoke, CsC, Customer-RP-discovery (Embedded-RP, AutoRP and BSR) are supported.
- Inter-AS Options A, B, and C are supported. VRF-Route-Import EC is announced in VPN-IP routes.

Profile 4: MS-PMSI-mLDP-MP2MP with BGP-AD

These are the characteristics of this profile:

- MP2MP mLDP trees are used in the core.
- The multicast traffic can be SM or SSM.
- Extranet, Hub and Spoke, CsC, Customer-RP-discovery (Embedded-RP, AutoRP, and BSR) are supported.
- Inter-AS Options A, B, and C are supported. VRF-Route-Import EC is announced in VPN-IP routes.

Profile 5: MS-PMSI-mLDP-P2MP with BGP-AD

These are the characteristics of this profile:

- P2MP mLDP trees are used in the core.
- The multicast traffic can be SM or SSM.
- Extranet, Hub and Spoke, CsC, Customer-RP-discovery (Embedded-RP, AutoRP, and BSR) are supported.
- Inter-AS Options A, B, and C are supported. VRF-Route-Import EC is announced in VPN-IP routes.

Profile 6: VRF In-band Signaling (No BGP-AD)

These are the characteristics of this profile:

- P2MP mLDP trees are used in the core.
• MoFRR in the core is supported.
• There is one core tree built per VRF-S,G route. There can be no (*,G) routes in VRF, with RPF reachability over the core.
• The multicast traffic can be SM S,G or SSM.

Profile 7: Global Inband Signalling

These are the characteristics of this profile:
• P2MP mLDP inband tree in the core; no C-multicast Routing.
• Customer traffic can be SM S,G or SSM.
• Support for global table S,Gs on PEs.

For more information on mLDP implementation and OAM concepts, see the Cisco IOS XR MPLS Configuration Guide for the Cisco ASR 9000 Series Router

Profile 8: Global P2MP-TE

These are the characteristics of this profile:
• P2MP-TE tree, with static Destination list, in the core; no C-multicast Routing.
• Static config of (S,G) required on Head-end PE.
• Only C-SSM support on PEs.
• Support for global table S,Gs on PEs.

Profile 9: Rosen-mLDP with BGP-AD

These are the characteristics of this profile:
• Single MP2MP mLDP core-tree as the Default-MDT, with PIM C-multicast Routing.
• All UMH options supported.
• Default and Data MDT supported.
• Customer traffic can be SM or SSM.
• RIB-Extranet, RPL-Extranet, Hub & Spoke supported.
• Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.

Profile 10: VRF Static-P2MP-TE with BGP AD

These are the characteristics of this profile:
• P2MP-TE tree, with static Destination list, in the core; no C-multicast Routing.
• Static config of (S,G) required on Head-end PE.
• Only C-SSM support on PEs.
• Support for IPv4 MVPN S,Gs on PEs. No support for IPv6 MVPN routes.
Profile 11: Rosen-PIM/GRE with BGP C-multicast Routing

These are the characteristics of this profile:

- PIM-trees in the core, data encapsulation is GRE, BGP C-multicast Routing.
- Static config of (S,G) required on Head-end PE.
- For PIM-SSM core-tree and PIM-SM core-tree with no spt-infinity, all UMH options are supported.
- For PIM-SM core-tree with spt-infinity case, only SFS (Highest PE or Hash-of-BGP-paths) is supported.
  Hash of installed-paths method is not supported.
- Default and Data MDTs supported.
- Customer traffic can be SM or SSM.
- Inter-AS Option A supported. Options B and C not supported.

Profile 12: Rosen-mLDP-P2MP with BGP C-multicast Routing

These are the characteristics of this profile:

- Full mesh of P2MP mLDP core-tree as the Default-MDT, with BGP C-multicast Routing.
- All UMH options supported.
- Default and Data MDT supported.
- Customer traffic can be SM or SSM.
- RPL-Tail-end-Extranet supported.
- Inter-AS Option A, B and C supported.

Profile 13: Rosen-mLDP-MP2MP with BGP C-multicast Routing

These are the characteristics of this profile:

- Single MP2MP mLDP core-tree as the Default-MDT, with BGP C-multicast Routing.
- Only SFS (Highest PE or Hash-of-BGP-paths) is supported. Hash of Installed-paths method is not supported.
- Default and Data MDT supported.
- Customer traffic can be SM or SSM.
- RIB-Tail-end-Extranet, RPL-Tail-end-Extranet supported.
- Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
- Inter-AS Option A, B and C supported. For Options B and C, Root has to be on a PE or the root-address reachability has to be leaked across all autonomous systems.

Profile 14: MP2MP-mLDP-P2MP with BGP C-multicast Routing

These are the characteristics of this profile:

- Full mesh of P2MP mLDP core-tree as the Default-MDT, with BGP C-multicast Routing.
- All UMH options supported.
Profile 15: MP2MP-mLDP-MP2MP with BGP C-multicast Routing

These are the characteristics of this profile:

- Full mesh of MP2MP mLDP core-tree as the Default-MDT, with BGP C-multicast Routing.
- All UMH options supported.
- Default and Data MDT supported.
- Customer traffic can be SM or SSM.
- RPL-Tail-end-Extranet supported.
- Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
- Inter-AS Option A, B and C supported.

Profile 16: Rosen-Static-P2MP-TE with BGP C-multicast Routing

These are the characteristics of this profile:

- Full mesh of Static-P2MP-TE core-trees, as the Default-MDT, with BGP C-multicast Routing.
- All UMH options supported.
- Support for Data MDT, Default MDT.
- Customer traffic can be SM, SSM.
- RPL-Tail-end-Extranet supported.
- Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
- Inter-AS Option A supported. Options B and C not supported.

Note
Whenever multicast stream crosses configured threshold on encap PE (Head PE), S-PMSI is announced. Core tunnel is static P2MP-TE tunnel configured under route-policy for the stream. Static P2MP-TE data mdt is implemented in such a way that it can work with dynamic data mdt, dynamic default mdt and default static P2MP.

Profile 17: Rosen-mLDP-P2MP with BGP AD/PIM C-multicast Routing

These are the characteristics of this profile:

- Full mesh of P2MP mLDP core-tree as the Default-MDT, with PIM C-multicast Routing.
- All UMH options supported.
• Default and Data MDT supported.
• Customer traffic can be SM or SSM.
• RPL-Extranet, Hub & Spoke supported.
• Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
• Inter-AS Option A, B and C supported.

Profile 18: Rosen-Static-P2MP-TE with BGP AD/PIM C-multicast Routing
These are the characteristics of this profile:
• Full mesh of Static-P2MP-TE core-trees, as the Default-MDT, with PIM C-multicast Routing.
• All UMH options supported.
• Default MDT supported; Data MDT is not supported.
• Customer traffic can be SM, SSM.
• RPL-Extranet, Hub & Spoke supported.
• Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
• Inter-AS Option A supported. Options B and C not supported.

Profile 20: Rosen-P2MP-TE with BGP AD/PIM C-multicast Routing
These are the characteristics of this profile:
• Dynamic P2MP-TE tunnels setup on demand, with PIM C-multicast Routing
• All UMH options supported.
• Default and Data MDT supported.
• Customer traffic can be SM, SSM.
• RPL-Extranet, Hub & Spoke supported.
• Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
• Inter-AS Option A and C supported.

Profile 22: Rosen-P2MP-TE with BGP C-multicast Routing
These are the characteristics of this profile:
• Dynamic P2MP-TE tunnels with BGP C-multicast Routing
• All UMH options supported.
• Default and Data MDT supported.
• Customer traffic can be SM or SSM.
• RIB-Tail-end-Extranet, RPL-Tail-end-Extranet supported.
• Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
Profile 24: Partitioned-P2MP-TE with BGP AD/PIM C-multicast Routing

These are the characteristics of this profile:

• Dynamic P2MP-TE tunnels setup on demand, with PIM C-multicast Routing
• All UMH options supported.
• Default and Data MDT supported.
• Customer traffic can be SM or SSM.
• RPL-Extranet, Hub & Spoke supported.
• Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
• Inter-AS Option A and C- supported.

Profile 26: Partitioned-P2MP-TE with BGP C-multicast Routing

These are the characteristics of this profile:

• Dynamic P2MP-TE tunnels with BGP C-multicast Routing
• All UMH options supported.
• Default and Data MDT supported.
• Customer traffic can be SM, SSM.
• RIB-Tail-end-Extranet, RPL-Tail-end-Extranet supported.
• Customer-RP-discovery (Embedded-RP, AutoRP & BSR) is supported.
• Inter-AS Option A and C- supported.

Configuration rules for profiles

Rules for Rosen-mGRE profiles (profiles- 0, 3, 11)

• All profiles require VPNv4 or v6 unicast reachability.
• By default, encap 1400-byte size c-multicast IP packet is supported. To support decap or encap larger packet size, `mdt mtu` command.
• Loopback configuration is required. Use the `mdt source loopback0` command. Other loopbacks can be used for different VRFs, but this is not recommended.

Rules for Rosen-mLDP profiles (profiles- 1, 9, 12, 13, 17)

• mLDP must be globally enabled.
• VPN-id is mandatory for Rosen-mLDP MP2MP profiles.
• Root node must be specified manually. Multiple root nodes can be configured for Root Node Redundancy.
• If only profile 1 is configured, MVPN must be enabled under bgp.
For BGP-AD profiles, the remote PE address is required.

Rules for mLDP profiles (profiles- 2, 4, 5, 14, 15)
- MVPN must be enabled under bgp, if only profile 2 is configured.
- Support only for static RP for customer RP.

Rules for inband mLDP profiles (profiles- 6, 7)
- MVPN must be enabled under bgp for vrf-inband profiles.
- Data MDT is not supported.
- Backbone facing interface (BFI) must be enabled on tail PE.
- Source route of SSM must be advertise to tail PE by iBGP.

MLDP inband signaling
MLDP Inband signaling allows the core to create (S,G) or (*,G) state without using out-of-band signaling such as BGP or PIM. It is supported in VRF (and in the global context). Both IPv4 and IPv6 multicast groups are supported.

In MLDP Inband signaling, one can configure an ACL range of multicast (S,G). This (S,G) can be transported in MLDP LSP. Each multicast channel (S,G), is 1 to 1 mapped to each tree in the inband tree. The (S,G) join, through IGMP/MLD/PIM, will be registered in MRIB, which is the client of MLDP.

MLDP In-band signalling supports transiting PIM (S,G) or (*,G) trees across a MPLS core without the need for an out-of-band protocol. In-band signaling is only supported for shared-tree-only forwarding (also known as sparse-mode threshold infinity). PIM Sparse-mode behavior is not supported (switching from (*,G) to (S,G)).

The details of the MLDP profiles are discussed in the *Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide*

### Summary of Supported MVPN Profiles
This tables summarizes the supported MVPN profiles:

<table>
<thead>
<tr>
<th>Profile Number</th>
<th>Name</th>
<th>Opaque-value</th>
<th>BGP-AD</th>
<th>Data-MDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Rosen GRE</td>
<td>N/A</td>
<td>N/A</td>
<td>PIM TLVs over default MDT</td>
</tr>
<tr>
<td>1</td>
<td>Rosen MLDP</td>
<td>Type 2 - Root Address:VPN-ID:0-n</td>
<td>N/A</td>
<td>PIM TLVs over default MDT</td>
</tr>
<tr>
<td>2</td>
<td>MS- PMSI (Partition) MLDP MP2MP</td>
<td>Cisco proprietary - Source- PE:RD:0</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>3</td>
<td>Rosen GRE with BGP-AD</td>
<td>N/A</td>
<td></td>
<td>PIM or BGP -AD (knob controlled)</td>
</tr>
</tbody>
</table>

*Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide, Release 4.2.x*
<table>
<thead>
<tr>
<th>Profile Number</th>
<th>Name</th>
<th>Opaque-value</th>
<th>BGP-AD</th>
<th>Data-MDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>MS- PMSI (Partition) MLDP MP2MP with BGP-AD</td>
<td>Type 1 - Source-PE:Global -ID</td>
<td>• I- PMSI with empty PTA</td>
<td>BGP-AD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• MS- PMSI for partition mdt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• S- PMSI for data-mdt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• S- PMSI cust RP-discovery trees</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>MS- PMSI (Partition) MLDP P2MP with BGP-AD</td>
<td>Type 1 - Source-PE:Global -ID</td>
<td>• I- PMSI with empty PTA</td>
<td>BGP-AD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• MS- PMSI for partition mdt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• S- PMSI for data-mdt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• S- PMSI cust RP-discovery trees</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>VRF Inband MLDP</td>
<td>RD:S,G</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>7</td>
<td>Global Inband</td>
<td>S,G</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>8</td>
<td>Global P2MP TE</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>9</td>
<td>Rosen MLDP with BGP-AD</td>
<td>Type 2 - RootAddresss:VPN - ID:0 -n</td>
<td>• Intra-AS MI- PMSI</td>
<td>PIM or BGP-AD</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• S- PMSI for Data-MDT</td>
<td>(knob controlled)</td>
</tr>
</tbody>
</table>

**Configuration Process for MLDP MVPN (Intranet)**

These steps provide a broad outline of the different configuration process of MLDP MVPN for intranet:

- Enabling MPLS MLDP
  - configure
• mpls ldp mldp

• Configuring a VRF entry
  • configure
  • vrf vrf_name
  • address-family ipv4/ipv6 unicast
  • import route-target route-target-ext-community
  • export route-target route-target-ext-community

• Configuring VPN ID
  • configure
  • vrf vrf_name
  • vpn id vpn_id

The configuring VPN ID procedure is needed for profiles 1 and 9 (Rosen MLDP).

• Configuring MVPN Routing and Forwarding instance
  • configure
  • multicast-routing vrf vrf_name
  • address-family ipv4
  • mdt default mldp ipv4 root-node

For profile 1 (MLDP Rosen), the mdt default mldp ipv4 command and for profile 4/5 (MS- PMSI with BGP-AD), the mdt partitioned mldp ipv4 mp2mp/p2mp command are configured.

• Configuring the Route Distinguisher
  • configure
  • router bgp AS Number
  • vrf vrf_name
  • rd rd_value

• Configuring Data MDTs (optional)
  • configure
  • multicast-routing vrf vrf_name
  • address-family ipv4
  • mdt data <1-255>

• Configuring BGP MDT address family
  • configure
  • router bgp AS Number
• Configuring BGP vpv4 address family
  * configure
  * router bgp AS Number
  * address-family vpv4 unicast

• Configuring BGP IPv4 VRF address family
  * configure
  * router bgp AS Number
  * vrf vrf_name
  * address-family ipv4 unicast

• Configuring PIM SM/SSM Mode for the VRFs
  * configure
  * router pim
  * vrf vrf_name
  * address-family ipv4
  * rpf topology route-policy rosen_mvpn_mldp

For each profile, a different route-policy is configured.

• Configuring route-policy
  * route-policy rosen_mvpn_mldp
  * set core-tree tree-type
  * pass
  * end-policy

For profile 1 (MLDP Rosen), the mldp-rosen core tree type and for profile 4/5 (MS- PMSI with BGP-AD), the mldp-partitioned-mp2mp/p2mp core tree type are configured.

---

**Note**

The configuration of the above procedures depends on the profile used for each configuration. For detailed examples of each profile, see Configuring LSM based MLDP: Examples, on page 227.

---

**MVPN over GRE**

A unicast GRE tunnel could be the accepting or forwarding interface for either a mVPN-GRE VRF route or a core route. When multicast packets arrive on the VRF interface with the intent of crossing the core, they are
first encapsulated with a multicast GRE header (S,G) which are applicable to the VRF’s MDT. Then, before the packets are actually forwarded, they are encapsulated in a unicast GRE header. The (S,D) in this packet are the origination and termination addresses for the unicast GRE tunnel.

GRE tunnel stitching is when both the accepting and forwarding interfaces are unicast GRE tunnels. Here, the packet has two GRE encapss. The outer encap is the unicast header for the GRE tunnel. The inner encap is the multicast GRE header for the MDT. This is called as double encap. There is a loss in terms of both bandwidth and throughput efficiency. The bandwidth efficiency loss is because 48 bytes of encap headers are being added to the original (VRF) packet. The throughput efficiency loss is the result of the processing time required to apply twoencaps.

For the mVPN-GRE, if the VRF interface is a GRE tunnel, the protocol packets received from LPTS will be accompanied with the receiving unicast GRE tunnel interface and the VRF id of the VRF in which the GRE tunnel is configured. Thus VRF specific processing can be done on the packet.

**Restrictions**

- MVPN over GRE is supported only on ASR 9000 Enhanced Ethernet LCs.

**Native Multicast**

GRE tunneling provides a method to transport native multicast traffic across a non-Multicast enabled IP network. Once the multicast traffic in encapsulated with GRE, it appears as an IP packet to the core transport network.

A GRE tunnel can be a forwarding interface when the router is the imposition (or encap) router for that GRE tunnel. The imposition router must prepend a unicast IPv4 header and GRE header to the multicast packet. The source and destination IPv4 addresses for the added header are determined by the user configuration of the tunnel. The newly encapsulated packet is then forwarded as a unicast packet.

When a GRE tunnel is an accepting interface for a multicast route, the router is the disposition (or decap) router for the tunnel. The outer IPv4 header and GRE header must be removed to expose the inner multicast packet. The multicast packet will then be forwarded just as any other multicast packet that arrives on a non-tunnel interface.

**Forwarding behavior**
Figure depicts a Unicast GRE tunnel between two routers. The imposition router has a multicast (S,G) route which has the GRE tunnel as a forwarding interface. At the disposition router, the GRE tunnel is an accepting interface for the multicast (S,G). As seen, the packet is unicast GRE encapsulated when it traverses the tunnel.

**Figure 11: Unicast GRE tunnel between two routers**

*Note*

Starting with IOS XR 5.3.2 release, IPv6 traffic is supported.

**GRE Limitations**

Listed below are the limitations for unicast GRE tunnels:

- GRE unicast tunnel supports IPv4 encapsulation only.

  *Note*

  Starting from the IOS XR 5.3.2 release, GRE unicast tunnels support IPv6 encapsulation.

- Native and mVPN traffic over underlying ECMP links are not supported.

  *Note*

  Starting with IOS XR 5.3.2 release, native and mVPN traffic over underlying ECMP links, including bundles is supported.

- IPv6 multicast for GRE unicast tunnels is not supported, in releases prior to IOS XR 5.3.2.
• Transport header support is limited to IPv4.
• Path MTU discovery will not be supported over GRE tunnel interfaces. When size of the packet going over GRE tunnel interface exceeds the tunnel MTU, the microcode will punt the packet to the slow path for best effort fragmentation. Since punted packets are policed, this doesn't provide real fragmentation support. This combined with no support for path MTU discovery means that user is responsible for making sure the MTUs configured along the tunnel path are large enough to guarantee the GRE packet will not be fragmented between tunnel source and destination routers.
• No support for optional checksum, key, and sequence number fields.
• No support for nested and concatenated GRE tunnels. If packets with nested GRE header are received they will be dropped.
• No L3 features (like QoS, ACL and netflow) support for GRE tunnel interfaces. Features configured on the underlying physical interface will be applied.
• ASR9000 SIP-700 linecard unicast GRE is NOT supported on VRFs.
• Support for up to 500 GRE tunnels per system for multicast.

Signaling and RPF on GRE Tunnels

Signaling will use the same mechanism when a unicast GRE tunnel terminated at an ingress linecard regardless of whether the GRE tunnel interface belongs to a VRF or not. In the case of mVPN-GRE the Master Linecard / Master NP mechanism must still be used for egress punts of decapsulated VRF packets.

RPF selection can be static configured via a route policy configuration. Static RPF is more preferred and expected if the RPF should be the GRE tunnel. RPF may be selected dynamically via RIB updates for the upstream router's unicast reach-ability, although this is not preferred.

PIM Registration

PIM registration packets can be forwarded on a unicast GRE tunnel as long as the IPv4 unicast GRE interface is selected by FIB for unicast forwarding of the encapsulated PIM registration packets toward the PIM RP. In this case, the packet is essentially double encapsulated with unicast, ie, the original multicast packet is encapsulated by PIM in a unicast PIM register packet. This is then encapsulated with the unicast GRE tunnel header.

At the PIM RP, outermost unicast header will be removed and the PIM registration packets will be delivered to PIM via LPTS as in the current PIM registration packet processing. It is advisable to avoid any MTU/TTL or ACL/QoS configuration issues that result in the registration packets getting dropped.

Auto-RP

Auto-RP lite on PEs, Auto-RP/BSR/static-RP/ Anycast-RP with MSDP peering etc can be supported over GRE tunnels with MFIB neto chain support. It is advisable to avoid any MTU/TTL or ACL/QoS configuration issues that result in the registration packets getting dropped. Auto-RP routes will flood autp-rp packets to every multicast egress interface including IPv4 unicast GRE tunnels.
Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP) is a mechanism to connect multiple PIM sparse-mode domains. MSDP allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains. Each PIM-SM domain uses its own RPs and need not depend on RPs in other domains.

An RP in a PIM-SM domain has MSDP peering relationships with MSDP-enabled routers in other domains. Each peering relationship occurs over a TCP connection, which is maintained by the underlying routing system.

MSDP speakers exchange messages called Source Active (SA) messages. When an RP learns about a local active source, typically through a PIM register message, the MSDP process encapsulates the register in an SA message and forwards the information to its peers. The message contains the source and group information for the multicast flow, as well as any encapsulated data. If a neighboring RP has local joiners for the multicast group, the RP installs the S, G route, forwards the encapsulated data contained in the SA message, and sends PIM joins back towards the source. This process describes how a multicast path can be built between domains.

Note

Although you should configure BGP or Multiprotocol BGP for optimal MSDP interdomain operation, this is not considered necessary in the Cisco IOS XR Software implementation. For information about how BGP or Multiprotocol BGP may be used with MSDP, see the MSDP RPF rules listed in the Multicast Source Discovery Protocol (MSDP), Internet Engineering Task Force (IETF) Internet draft.

VRF-aware MSDP

VRF (VPN Routing and Forwarding) -aware MSDP enables MSDP to function in the VRF context. This in turn, helps the user to locate the PIM (protocol Independent Multicast) RP on the Provider Edge and use MSDP for anycast-RP.

MSDP needs to be VRF-aware when:

- Anycast-RP is deployed in an MVPN (Multicast MVPN) in such a manner that one or more PIM RPs in the anycast-RP set are located on a PE. In such a deployment, MSDP needs to operate in the VRF context on the PE.
- The PIM RP is deployed in an MVPN in such a manner that it is not on a PE and when the customer multicast routing type for the MVPN is BGP and the PEs have suppress-shared-tree-join option configured. In this scenario, there is no PE-shared tree link, so traffic may stop at the RP and it does not flow to other MVPN sites. An MSDP peering between the PIM RP and one or more PEs resolves the issue.

Multicast Nonstop Forwarding

The Cisco IOS XR Software nonstop forwarding (NSF) feature for multicast enhances high availability (HA) of multicast packet forwarding. NSF prevents hardware or software failures on the control plane from disrupting the forwarding of existing packet flows through the router.

The contents of the Multicast Forwarding Information Base (MFIB) are frozen during a control plane failure. Subsequently, PIM attempts to recover normal protocol processing and state before the neighboring routers time out the PIM hello neighbor adjacency for the problematic router. This behavior prevents the NSF-capable router from being transferred to neighbors that will otherwise detect the failure through the timed-out adjacency.
Routes in MFIB are marked as stale after entering NSF, and traffic continues to be forwarded (based on those routes) until NSF completion. On completion, MRIB notifies MFIB and MFIB performs a mark-and-sweep to synchronize MFIB with the current MRIB route information.

**Multicast Configuration Submodes**

Cisco IOS XR Software moves control plane CLI configurations to protocol-specific submodes to provide mechanisms for enabling, disabling, and configuring multicast features on a large number of interfaces.

Cisco IOS XR Software allows you to issue most commands available under submodes as one single command string from the global or XR config mode.

For example, the `ssm` command could be executed from the multicast-routing configuration submode like this:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast-ipv4)# ssm range
```

Alternatively, you could issue the same command from the global or XR config mode like this:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing ssm range
```

The following multicast protocol-specific submodes are available through these configuration submodes:

**Multicast-Routing Configuration Submode**

In Cisco IOS XR software release 3.7.2 and later, basic multicast services start automatically when the multicast PIE (asr9k-mcast-p.pie) is installed, without any explicit configuration required. The following multicast services are started automatically:

- MFWD
- MRIB
- PIM
- IGMP

Other multicast services require explicit configuration before they start. For example, to start the MSDP process, you must enter the `router msdp` command and explicitly configure it.

When you issue the `multicast-routing ipv4` or `multicast-routing ipv6` command, all default multicast components (PIM, IGMP, MLD, MFWD, and MRIB) are automatically started, and the CLI prompt changes to "config-mcast-ipv4" or "config-mcast-ipv6", indicating that you have entered multicast-routing configuration submode.

**PIM Configuration Submode**

When you issue the `router pim` command, the CLI prompt changes to "config-pim-ipv4," indicating that you have entered the default pim address-family configuration submode.

To enter pim address-family configuration submode for IPv6, type the `address-family ipv6` keyword together with the `router pim` command before pressing Enter.
**IGMP Configuration Submode**

When you issue the `router igmp` command, the CLI prompt changes to “config-igmp,” indicating that you have entered IGMP configuration submode.

**MLD Configuration Submode**

When you issue the `router mld` command, the CLI prompt changes to “config-mld,” indicating that you have entered MLD configuration submode.

**MSDP Configuration Submode**

When you issue the `router msdp` command, the CLI prompt changes to “config-msdp,” indicating that you have entered router MSDP configuration submode.

**Understanding Interface Configuration Inheritance**

Cisco IOS XR Software allows you to configure commands for a large number of interfaces by applying command configuration within a multicast routing submode that could be inherited by all interfaces. To override the inheritance mechanism, you can enter interface configuration submode and explicitly enter a different command parameter.

For example, in the following configuration you could quickly specify (under router PIM configuration mode) that all existing and new PIM interfaces on your router will use the hello interval parameter of 420 seconds. However, Packet-over-SONET/SDH (POS) interface 0/1/0/1 overrides the global interface configuration and uses the hello interval time of 210 seconds.

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# hello-interval 420
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/1
RP/0/RSP0/CPU0:router(config-pim-ipv4-if)# hello-interval 210
```

The following is a listing of commands (specified under the appropriate router submode) that use the inheritance mechanism:

```
router pim
  dr-priority
  hello-interval
  join-prune-interval

multicast-routing
  version
  query-interval
  query-max-response-time
  explicit-tracking
router mld
  interface all disable
  version
  query-interval
  query-max-response-time
  explicit-tracking

router msdp
  connect-source
  sa-filter
```
Understanding Interface Configuration Inheritance Disablement

As stated elsewhere, Cisco IOS XR Software allows you to configure multiple interfaces by applying configurations within a multicast routing submodule that can be inherited by all interfaces.

To override the inheritance feature on specific interfaces or on all interfaces, you can enter the address-family IPv4 or IPv6 submodule of multicast routing configuration mode, and enter the `interface-inheritance disable` command together with the `interface type interface-path-id` or `interface all` command. This causes PIM or IGMP protocols to disallow multicast routing and to allow only multicast forwarding on those interfaces specified. However, routing can still be explicitly enabled on specified individual interfaces.

The following configuration disables multicast routing interface inheritance under PIM and IGMP generally, although forwarding enablement continues. The example shows interface enablement under IGMP of GigabitEthernet 0/6/0/3:

```
RP/0/RSP0/CPU0:router# multicast-routing address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface-inheritance disable
```

For related information, see Understanding Enabling and Disabling Interfaces, on page 99

Understanding Enabling and Disabling Interfaces

When the Cisco IOS XR Software multicast routing feature is configured on your router, by default, no interfaces are enabled.

To enable multicast routing and protocols on a single interface or multiple interfaces, you must explicitly enable interfaces using the `interface` command in multicast routing configuration mode.

To set up multicast routing on all interfaces, enter the `interface all` command in multicast routing configuration mode. For any interface to be fully enabled for multicast routing, it must be enabled specifically (or be default) in multicast routing configuration mode, and it must not be disabled in the PIM and IGMP/MLD configuration modes.

For example, in the following configuration, all interfaces are explicitly configured from multicast routing configuration submodule:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# interface all enable
```
To disable an interface that was globally configured from the multicast routing configuration submode, enter interface configuration submode, as illustrated in the following example:

```
RP/0/RSP0/CPU0:router(config-mcast)# interface GigabitEthernet0/0/1/0
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4-if)# disable
```

### Multicast Routing Information Base

The Multicast Routing Information Base (MRIB) is a protocol-independent multicast routing table that describes a logical network in which one or more multicast routing protocols are running. The tables contain generic multicast routes installed by individual multicast routing protocols. There is an MRIB for every logical network (VPN) in which the router is configured. MRIBs do not redistribute routes among multicast routing protocols; they select the preferred multicast route from comparable ones, and they notify their clients of changes in selected attributes of any multicast route.

### Multicast Forwarding Information Base

Multicast Forwarding Information Base (MFIB) is a protocol-independent multicast forwarding system that contains unique multicast forwarding entries for each source or group pair known in a given network. There is a separate MFIB for every logical network (VPN) in which the router is configured. Each MFIB entry resolves a given source or group pair to an incoming interface (IIF) for reverse forwarding (RPF) checking and an outgoing interface list (olist) for multicast forwarding.

### MSDP MD5 Password Authentication

MSDP MD5 password authentication is an enhancement to support Message Digest 5 (MD5) signature protection on a TCP connection between two Multicast Source Discovery Protocol (MSDP) peers. This feature provides added security by protecting MSDP against the threat of spoofed TCP segments being introduced into the TCP connection stream.

MSDP MD5 password authentication verifies each segment sent on the TCP connection between MSDP peers. The `password clear` command is used to enable MD5 authentication for TCP connections between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified.

**Note**

MSDP MD5 authentication must be configured with the same password on both MSDP peers to enable the connection between them. The `password encrypted` command is used only for applying the stored running configuration. Once you configure the MSDP MD5 authentication, you can restore the configuration using this command.

MSDP MD5 password authentication uses an industry-standard MD5 algorithm for improved reliability and security.
Overriding VRFs in IGMP Interfaces

All unicast traffic on the user-to-network interfaces of next-generation aggregation or core networks must be mapped to a specific VRF. They must then be mapped to an MPLS VPN on the network-to-network side. This requires the configuration of a physical interface in this specific VRF.

This feature allows mapping of IGMP packets entering through a user-to-user interface to the multicast routes in the global multicast routing table. This ensures that the interface in a specific VRF can be part of the outgoing list of interfaces in the table for a multicast route.

IGMP packets entering through a non-default VRF interface in the default (global) VRF are processed, with IGMP later distributing the interface-related multicast state (route/interface) to MRIB. This occurs through the default VRF rather than through the VRF to which the interface belongs. MRIB, PIM, MSDP, and MFIB then process the multicast state for this interface through the default VRF.

When an IGMP join for a specific \((S,G)\) is received on the configured interface, IGMP stores this information in its VRF-specific databases. But, when sending an update to MRIB, IGMP sends this route through the default VRF. MRIB then programs this \((S,G)\) along with this interface as an OLIST member in the default multicast routing table.

Similarly, when PIM requests information about IGMP routes from MRIB, MRIB sends this update to PIM in the context of the default VRF.

This feature specifically supports:

- Mapping of IGMP requests on an interface in a non-default VRF to the default VRF multicast routing table.
- Enabling and disabling of VRF override functionality at run time.
- Routing policy configuration at the global (default) VRF level, because routing policy configuration cannot be done at the granularity of an individual interface.
- Enablement and disablement of an IGMP VRF override on all Layer-3 and Layer-2 interface types, including physical Ethernet, VLAN sub-interface, bundles and VLANs over bundles.
- The same scale of multicast routes and OLIST interfaces currently supported by the platform even when VRF override functionality is operational.

VRF support for MLD

MLD receives MLD joins, membership queries and membership reports under VRF. The MLD process will have LPTS entries per VRF and traffic is redirected based on the matching VRF entry to the correct interface configured under the given VRF. Support for Source-Specific Multicast (SSM) is also provided under VRF.

Support for Satellite nV

Multicast components, which include IGMP, IGMP Snooping, PIM, MRIB/LMRIB, MFIB, L2FIB, are enhanced to recognize the new Satellite-Ether interface type and to also query and maintain the logical or physical type.
How to Implement Multicast Routing

This section contains instructions for both building a basic multicast configuration, as well as optional tasks to help you to optimize, debug, and discover the routers in your multicast network.

Configuring PIM-SM and PIM-SSM

SUMMARY STEPS

1. configure
2. multicast-routing [address-family {ipv4 | ipv6}]
3. interface all enable
4. exit
5. Use `router igmp` for IPv4 hosts or use `router mld` for IPv6
6. version {1 | 2 | 3} for IPv4 (IGMP) hosts or version {1 | 2} for IPv6 (MLD) hosts.
7. commit
8. show pim [ipv4 | ipv6] group-map [ip-address-name] [info-source]
9. show pim [vrf vrf-name] [ipv4 | ipv6] topology [source-ip-address [group-ip-address] | entry-flag flag | interface-flag | summary] [route-count]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>multicast-routing [address-family {ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing</td>
</tr>
</tbody>
</table>

Enters multicast routing configuration mode.

- The following multicast processes are started: MRIB, MFWD, PIM, and IGMP.
- For IPv4, IGMP version 3 is enabled by default.
## Purpose

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>interface all enable</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-ipv4)# interface all enable</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Exits multicast routing configuration mode, and returns the router to the source configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-ipv4)# exit</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Use <code>router igmp</code> for IPv4 hosts or use <code>router mld</code> for IPv6</td>
<td>(Optional) Enters router IGMP configuration mode (for IPv4 hosts), or enters router MLD configuration mode (for IPv6 hosts).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router igmp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router mld</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>`version {1</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-igmp)# version 3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mld)# version 2</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>commit</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>`show pim [ipv4</td>
<td>ipv6] group-map [ip-address-name] [info-source]`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router# show pim ipv4 group-map</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>`show pim [vrf vrf-name] [ipv4</td>
<td>ipv6] topology [source-ip-address [group-ip-address]</td>
</tr>
</tbody>
</table>

### Notes

- The version range for IGMP is 1-3; the range for MLD is 1-2.
- The default for IGMP is version 3; the default for MLD is version 1.
- Host receivers must support IGMPv3 for PIM-SSM operation.
- If this command is configured in router IGMP or router MLD configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode.
Deploying PIM-SSM in legacy multicast-enabled networks can be problematic, because it requires changes to the multicast group management protocols used on the various devices attached to the network. Host, routers, and switches must all be upgraded in such cases.

To support legacy hosts and switches in a PIM-SSM deployment, Cisco ASR 9000 Series Routers offer a configurable mapping feature. Legacy group membership reports for groups in the SSM group range are mapped to a set of sources providing service for that set of (S,G) channels.

This configuration consists of two tasks:

**Restrictions for PIM-SSM Mapping**

PIM-SSM mapping does not modify the SSM group range. Instead, the legacy devices must report group membership for desired groups in the SSM group range.

**Configuring a Set of Access Control Lists for Static SSM Mapping**

This task configures a set of access control lists (ACLs) where each ACL describes a set of SSM groups to be mapped to one or more sources.

**SUMMARY STEPS**

1. configure
2. ipv4 access-list acl-name
3. [sequence-number] permit source [source-wildcard]
4. Repeat Step 3, on page 105 to add more entries to the ACL.
5. Repeat Step 2, on page 105 through Step 4, on page 105 until you have entered all the ACLs you want to be part of the set.
6. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
</tbody>
</table>
Configuring a Set of Sources for SSM Mapping

This task consists of configuring a set of sources mapped by SSM groups, as described by access lists (ACLs).

**SUMMARY STEPS**

1. configure
2. router igmp [vrf vrf-name]
3. ssm map static source-address access-list
4. Repeat Step 3, on page 106 as many times as you have source addresses to include in the set for SSM mapping.
5. commit
6. show igmp [vrf vrf-name] ssm map [group-address][detail]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 router igmp [vrf vrf-name]</td>
<td>Enters router IGMP configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router igmp vrf vrf20</td>
</tr>
</tbody>
</table>
### Configuring a Static RP and Allowing Backward Compatibility

When PIM is configured in sparse mode, you must choose one or more routers to operate as a rendezvous point (RP) for a multicast group. An RP is a single common root placed at a chosen point of a shared distribution tree. An RP can either be configured statically in each router, or learned through Auto-RP or BSR.

This task configures a static RP. For more information about RPs, see the Rendezvous Points, on page 66. For configuration information for Auto-RP, see the Configuring Auto-RP to Automate Group-to-RP Mappings, on page 108.

#### SUMMARY STEPS

1. configure
2. router pim [address-family {ipv4 | ipv6}]
3. rp-address ip-address [group-access-list] [bidir] [override]
4. old-register-checksum
5. exit
6. {ipv4 | ipv6} access-list name
7. [sequence-number] permit source [source-wildcard]
8. commit

### Command or Action

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>ssm map static source-address access-list</td>
<td>Configures a source as part of a set of sources that map SSM groups described by the specified access list.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-igmp)# ssm map static 232.1.1.1 mc2</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Repeat Step 3, on page 106 as many times as you have source addresses to include in the set for SSM mapping.</td>
<td>—</td>
</tr>
<tr>
<td>Step 5</td>
<td>commit</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>show igmp [vrf vrf-name] ssm map [group-address][detail]</td>
<td>(Optional) Queries the mapping state.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router# show igmp vrf vrf20 ssm map 232.1.1.1</td>
<td>232.1.1.1 is static with 1 source or</td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router# show igmp vrf vrf20 ssm map 232.1.1.0 is static with 3 sources</td>
<td>232.1.1.1 is static with 1 source</td>
</tr>
</tbody>
</table>
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters PIM configuration mode, or PIM address-family configuration submode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# router pim</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Assigns an RP to multicast groups.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# rp-address 172.16.6.22 rp-access</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>(Optional) Allows backward compatibility on the RP that uses old register checksum methodology.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-pim-ipv4)# old-register-checksum</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Exits PIM configuration mode, and returns the router to the source configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-pim-ipv4)# exit</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Enters access list configuration mode and configures the RP access list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-pim-ipv4-acl)# ipv4 access-list rp-access</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>(Optional) Permits multicast group 239.1.1.0 0.0.255.255 for the “rp-access” list.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-pim-ipv4-acl)# permit 239.1.1.0 0.0.255.255</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>
Configuring Auto-RP to Automate Group-to-RP Mappings

This task configures the Auto-RP mechanism to automate the distribution of group-to-RP mappings in your network. In a network running Auto-RP, at least one router must operate as an RP candidate and another router must operate as an RP mapping agent. The VRF interface on Cisco ASR 9000 Series Routers cannot be an auto-rp candidate rp.

SUMMARY STEPS

1. configure
2. router pim [address-family ipv4]
3. auto-rp candidate-rp type instance scope ttl-value [group-list access-list-name] [interval seconds] bidir
4. auto-rp mapping-agent type number scope ttl-value [interval seconds]
5. exit
6. ipv4 access-list name
7. [sequence-number] permit source [source-wildcard]
8. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters PIM configuration mode, or PIM address-family configuration submode.</td>
</tr>
<tr>
<td>Step 2 router pim [address-family ipv4]</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# router pim</td>
<td></td>
</tr>
<tr>
<td>Step 3 auto-rp candidate-rp type instance scope ttl-value [group-list access-list-name] [interval seconds] bidir</td>
<td>Configures an RP candidate that sends messages to the CISCO-RP-ANNOUNCE multicast group (224.0.1.39).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-ipv4)# auto-rp candidate-rp GigabitEthernet0/1/0/1 scope 31 group-list 2 bidir</td>
<td></td>
</tr>
<tr>
<td>Step 4 auto-rp mapping-agent type number scope ttl-value [interval seconds]</td>
<td>Configures the router to be an RP mapping agent on a specified interface.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-ipv4)#</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| auto-rp mapping-agent GigabitEthernet0/1/0/1 scope 20 | the mappings in an Auto-RP discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40).  
  - A PIM DR listens to this well-known group to determine which RP to use.  
  - This example limits Auto-RP discovery messages to 20 hops. |

**Step 5**  
**Example:**  
RP/0/RSP0/CP00:router(config-pim-ipv4)# exit  
**Purpose:** Exits PIM configuration mode and returns the router to the source configuration mode.

**Step 6**  
**Optional**  
**Example:**  
RP/0/RSP0/CP00:router(config)# ipv4 access-list 2  
**Purpose:** (Optional) Defines the RP access list.

**Step 7**  
**Optional**  
**Example:**  
RP/0/RSP0/CP00:router(config-ipv4-acl)# permit 239.1.1.1 0.0.0.0  
**Purpose:** (Optional) Permits multicast group 239.1.1.1 for the RP access list.  
**Tip** The commands in **Step 6, on page 109** and **Step 7, on page 109** can be combined in one command string and entered from the global or XR config mode like this: ipv4 access-list rp-access permit 239.1.1.1 0.0.0.0

**Step 8**  
**commit**

### Configuring the Bootstrap Router

This task configures one or more candidate bootstrap routers (BSRs) and a BSR mapping agent. This task also connects and locates the candidate BSRs in the backbone portion of the network.

For more information about BSR, see the PIM Bootstrap Router, on page 68.
SUMMARY STEPS

1. configure
2. router pim [address-family {ipv4 | ipv6}]
3. bsr candidate-bsr ip-address [hash-mask-len length] [priority value]
4. bsr candidate-rp ip-address [group-list access-list interval seconds] [priority value] bidir
5. interface type interface-path-id
6. bsr-border
7. exit
8. exit
9. {ipv4 | ipv6} access-list name
10. Do one of the following:
   • [sequence-number] permit source [source-wildcard]
   • [sequence-number] permit source-prefix dest-prefix
11. commit
12. clear pim [vrf vrf-name] [ipv4 | ipv6] bsr
13. show pim [vrf vrf-name] [ipv4 | ipv6] bsr candidate-rp
14. show pim [vrf vrf-name] [ipv4 | ipv6] bsr election
15. show pim [vrf vrf-name][ipv4 | ipv6] bsr rp-cache
16. show pim [vrf vrf-name][ipv4 | ipv6] group-map [ip-address-name] [info-source]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
<td>Enters PIM configuration mode, or address-family configuration submode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router pim [address-family {ipv4</td>
<td>ipv6}]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# router pim</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>bsr candidate-bsr ip-address [hash-mask-len length] [priority value]</td>
<td>Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-bsr 10.0.0.1 hash-mask-len 30</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>bsr candidate-rp ip-address [group-list access-list interval seconds] [priority value] bidir</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-default-ipv4)#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bsr candidate-rp 172.16.0.0 group-list 4 bidir</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface type interface-path-id</td>
<td>(Optional) Enters interface configuration mode for the PIM protocol.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-default-ipv4)#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface GigE 0/1/0/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> bsr-border</td>
<td>(Optional) Stops the forwarding of bootstrap router (BSR) messages on</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>a Protocol Independent Multicast (PIM) router interface.</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-ipv4-if)#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bsr-border</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>(Optional) Exits PIM interface configuration mode, and returns the</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>router to PIM configuration mode.</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-ipv4-if)#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> exit</td>
<td>Exits PIM configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-default-ipv4)#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> {ipv4</td>
<td>ipv6} access-list name</td>
<td>(Optional) Defines the candidate group list to the BSR.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# ipv4 access-list 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>{ipv4</td>
<td>ipv6} access-list name</td>
<td></td>
</tr>
<tr>
<td>{ipv4</td>
<td>ipv6} access-list name</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> Do one of the following:</td>
<td>(Optional) Permits multicast group 239.1.1.1 for the candidate group</td>
<td></td>
</tr>
<tr>
<td>• [sequence-number] permit source [source-wildcard]</td>
<td>list.</td>
<td></td>
</tr>
<tr>
<td>• [sequence-number] permit source-prefix dest-prefix</td>
<td>Tip The commands in Step 6, on page 111 and Step 7, on page 111 can</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>be combined in one command string and entered from global configuration</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit</td>
<td>mode like this: ipv4 access-list rp-access permit 239.1.1.1 0.255.255.255</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>239.1.1.1 0.255.255.255</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>commit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>clear pim [vrf vrf-name] [ipv4</td>
<td>ipv6] bsr</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Clears BSR entries from the PIM RP group mapping cache.</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# clear pim bsr</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>show pim [vrf vrf-name] [ipv4</td>
<td>ipv6] bsr candidate-rp</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Displays PIM candidate RP information for the BSR.</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# show pim bsr candidate-rp</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>show pim [vrf vrf-name] [ipv4</td>
<td>ipv6] bsr election</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Displays PIM candidate election information for the BSR.</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# show pim bsr election</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong></td>
<td>show pim [vrf vrf-name][ipv4</td>
<td>ipv6] bsr rp-cache</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Displays PIM RP cache information for the BSR.</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# show pim bsr rp-cache</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 16</strong></td>
<td>show pim [vrf vrf-name][ipv4</td>
<td>ipv6] group-map [ip-address-name] [info-source]</td>
</tr>
<tr>
<td>Example:</td>
<td>(Optional) Displays group-to-PIM mode mapping.</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router# show pim ipv4 group-map</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Calculating Rates per Route

This procedure enables multicast hardware forward-rate counters on a per-VRF-family basis.
SUMMARY STEPS

1. configure
2. multicast-routing [vrf vrf-name] [address-family {ipv4 | ipv6}]
3. rate-per-route
4. interface {type interface-path-id | all} enable
5. Do one of the following:
   • accounting per-prefix
   • accounting per-prefix forward-only
6. commit
7. show mfib [vrf vrf-name] [ipv4 | ipv6] route [rate | statistics] [* | source-address] [group-address [prefix-length] [detail | old-output] | summary] [location node-id]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>multicast-routing [vrf vrf-name] [address-family {ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing address-family ipv4</td>
</tr>
<tr>
<td></td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td></td>
<td>• The following multicast processes are started: MRIB, MFWD, PIM, and IGMP.</td>
</tr>
<tr>
<td></td>
<td>• For IPv4, IGMP version 3 is enabled by default.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>rate-per-route</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# rate-per-route</td>
</tr>
<tr>
<td></td>
<td>Enables a per (S,G) rate calculation for a particular route.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>interface {type interface-path-id</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface FastEthernet0/3/3/1 enable</td>
</tr>
<tr>
<td></td>
<td>Enables multicast routing on all interfaces.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• accounting per-prefix</td>
</tr>
<tr>
<td></td>
<td>• Enables per-prefix counters present in hardware, assigning every existing and new (S, G) route forward, punt, and drop counters on the ingress route and forward</td>
</tr>
</tbody>
</table>
Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting per-prefix forward-only</td>
<td>and punt counters on the egress route. The (*) G) routes are assigned a single counter.</td>
</tr>
<tr>
<td>Example:</td>
<td>Enables per-prefix counters present in hardware accounting per-prefix Enables three counters on ingress (forward, punt and drop, and two on egress (forward and punt) on every existing and new (S, G) route. The (*, G) routes are assigned a single counter.</td>
</tr>
<tr>
<td>accounting per-prefix forward-only</td>
<td>Enables one counter on ingress and one on egress in hardware to conserve hardware statistics resources. (Recommended for configuration of multicast VPN routing or for any line card that has a route-intensive configuration.)</td>
</tr>
</tbody>
</table>

Step 6

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>commit</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB) table.</td>
</tr>
</tbody>
</table>

Step 7

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib [vrf vrf-name] [ipv4</td>
<td>ipv6] route [rate</td>
</tr>
<tr>
<td>Example:</td>
<td>When the statistics keyword is used, the command displays the rate per route for one line card in the Multicast Forwarding Information Base (MFIB) table.</td>
</tr>
</tbody>
</table>

Configuring Multicast Nonstop Forwarding

This task configures the nonstop forwarding (NSF) feature for multicast packet forwarding for the purpose of alleviating network failures, or software upgrades and downgrades.

Although we strongly recommend that you use the NSF lifetime default values, the optional Step 3, on page 115 through Step 6, on page 116 allow you to modify the NSF timeout values for Protocol Independent Multicast (PIM) and Internet Group Management Protocol (IGMP) or Multicast Listener Discovery (MLD). Use these commands when PIM and IGMP (or MLD) are configured with nondefault interval or query intervals for join and prune operations.

Generally, configure the IGMP NSF and PIM NSF lifetime values to equal or exceed the query or join query interval. For example, if you set the IGMP query interval to 120 seconds, set the IGMP NSF lifetime to 120 seconds (or greater).

If the Cisco IOS XR Software control plane does not converge and reconnect after NSF is enabled on your router, multicast packet forwarding continues for up to 15 minutes, then packet forwarding stops.
Before You Begin

For NSF to operate in your multicast network, you must also enable NSF for the unicast protocols (such as IS-IS, OSPF, and BGP) that PIM relies on for Reverse Path Forwarding (RPF) information. See the appropriate configuration modules to learn how to configure NSF for unicast protocols.

SUMMARY STEPS

1. configure
2. router pim [address-family {ipv4 | ipv6}]
3. nsf lifetime seconds
4. exit
5. router {igmp | mld}
6. nsf lifetime seconds
7. commit
8. show {igmp nsf
9. show mfib [ipv4 | ipv6] nsf [location node-id]
10. show mrib [ipv4 | ipv6] nsf
11. show pim [ipv4 | ipv6] nsf

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>nsf lifetime seconds</td>
<td>(Optional) Enters PIM address-family configuration submode.</td>
</tr>
</tbody>
</table>

Example:

RP/0/RSP0/CPU0:router(config)# router pim address-family ipv4

Example:

RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# nsf lifetime 30

Note
If you configure the PIM hello interval to a nondefault value, configure the PIM NSF lifetime to a value less than the hello hold time. Typically the value of the hold-time field is 3.5 times the interval time value, or 120 seconds if the PIM hello interval time is 30 seconds.

Step 4 | exit | (Optional) Exits PIM configuration mode and returns the router to the source configuration mode. |

Example:

RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# exit
## Configuring Multicast VPN

- **Enabling a VPN for Multicast Routing**, on page 118 (required)
- “Configuring BGP to Advertise VRF Routes for Multicast VPN from PE to PE” (required)

See the module “Implementing BGP on Cisco IOS XR Software in *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*.”

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>`router [igmp</td>
<td>mld]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config)# router igmp</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>nsf lifetime seconds</code></td>
<td>(Optional) Configures the NSF timeout value for multicast forwarding route entries under the IGMP process.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router(config-igmp)# nsf lifetime 30</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>commit</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>show [igmp nsf]</code></td>
<td>(Optional) Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router# show igmp nsf</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>`show mfib [ipv4</td>
<td>ipv6] nsf [location node-id]`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router# show mfib nsf</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>`show mrib [ipv4</td>
<td>ipv6] nsf`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router# show mrib nsf</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td>`show pim [ipv4</td>
<td>ipv6] nsf`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>RP/0/RSP0/CPU0:router# show pim nsf</code></td>
<td></td>
</tr>
</tbody>
</table>
• Configuring an MDT Address Family Session in BGP as a PE-to-PE Protocol (optional for PIM-SM MDT groups; required for PIM-SSM MDT groups)

See the "Configuring an MDT Address Family Session in BGP" section in *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*.

• Configuring a provider-edge-to-customer-edge protocol (optional)


• Specifying the PIM VRF Instance, on page 120 (optional)

### Prerequisites for Multicast VPN

• PIM and multicast forwarding must be configured on all interfaces used by multicast traffic. In an MVPN, you must enable PIM and multicast forwarding for the following interfaces:
  - Physical interface on a provider edge (PE) router that is connected to the backbone.
  - Interface used for BGP peering source address.
  - Any interfaces configured as PIM rendezvous points.

| Note | PIM and multicast forwarding are enabled in multicast routing configuration mode. No additional configuration is required in router pim mode to enable the PIM protocol. |

• Interfaces in the VPN intended for use in forwarding multicast traffic must be enabled for PIM and multicast forwarding.

• BGP should already be configured and operational on all routers that are sending or receiving multicast traffic.

• To enable MVPN, you must include a VPN IPv4 address-family (AFI) in your BGP configuration. See *Restrictions for Multicast VPN for Multicast Routing*, on page 117. (See also the "Enabling BGP Routing" section in Cisco IOS XR Routing Configuration Guide.)

• All PE routers in the multicast domain must be running a Cisco IOS XR Software image that supports MVPN.

• Multicast forwarding must be configured for the global IPv4 address family.

• Each multicast SM VRF domain must have an associated PIM rendezvous point (RP) definition. Using Auto-RP and the bootstrap router (BSR), you may configure RP services in the MVPN on the customer-edge (CE) device because the MVPN learns about the RP dynamically. The VRF interface can be used as a listener on the PE device.

To enable static RP services, you must configure every device in the domain for this purpose.

### Restrictions for Multicast VPN for Multicast Routing

• Configuration of the MDT source on a per-VRF basis is only supported on IPv4.
• The MDT group address should be the same for both the address families in the same VRF.

Enabling a VPN for Multicast Routing

This task enables multicast VPN routing for IPv4.

The MDT group address is used by provider edge (PE) routers to form a virtual PIM "neighborship" for the MDT. This enables the PEs to communicate with other PEs in the VRF as if they shared a LAN.

When sending customer VRF traffic, PEs encapsulate the traffic in their own (S,G) state, where the G is the MDT group address, and the S is the MDT source for the PE. By joining the (S,G) MDT of its PE neighbors, a PE router is able to receive the encapsulated multicast traffic for that VRF.

Although the VRF itself may have many multicast sources sending to many groups, the provider network needs only to install state for one group per VRF, in other words, the MDT group.

SUMMARY STEPS

1. configure
2. multicast-routing
3. address-family ipv4
4. nsf
5. mdt source type interface-path-id
6. interface all enable
7. vrf vrf-name
8. address-family {ipv4}]
9. mdt default mdt-group-address
10. mdt data mdt-group-address/prefix-length threshold threshold acl-name
11. mdt mtu size
12. interface all enable
13. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>multicast-routing</td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/GPU0:router(config)# multicast-routing</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>address-family ipv4</td>
<td>Enters ipv4 address-family submode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/GPU0:router(config-mcast)#</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>address-family ipv4</td>
<td>Specifies that nonstop forwarding (NSF) maintains the forwarding state in case of a disruption to a multicast process.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**  
**nsf**  
**Example:**  

```
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# nsf
```

**Step 5**  
**mdt source type interface-path-id**  
**Example:**  

```
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# mdt source GigE 0/1/0/0
```

**Step 6**  
**interface all enable**  
**Example:**  

```
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable
```

**Step 7**  
**vrf vrf-name**  
**Example:**  

```
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# vrf vrf_A
```

**Step 8**  
**address-family {ipv4}**  
**Purpose:** Specifies the virtual routing and forwarding instance for the ipv4 address family.  

**Step 9**  
**mdt default mdt-group-address**  
**Example:**  

```
RP/0/RSP0/CPU0:router(config-mcast-vrf_A-ipv4)# mdt default 239.23.2.1
```

**Step 10**  
**mdt data mdt-group-address/prefix-length threshold threshold acl-name**  
**Example:**  

```
RP/0/RSP0/CPU0:router(config-mcast-vrf_A-ipv4)# mdt data 239.23.3.0/24 threshold 1200 acl-A
```

**Note**: This group range should not overlap the MDT default group. This is an optional command. The default threshold beyond which traffic is sent using a data MDT group is 1 kbps. However, you may configure a higher threshold, if desired. You may also, optionally, configure an access list to limit the number of groups to be tunneled through a data MDT.
### Purpose Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>group. Traffic from groups not on the access-list continues to be tunneled using the default MDT group.</td>
</tr>
</tbody>
</table>

#### Step 11

**mdt mtu size**

**Example:**

```
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)#
mtd mtu 1550
```

This is an optional step.

Specifies the MTU size. It is recommended to configure a high value, to accommodate the maximum multicast packet size.

**Note**
The default MTU for PIM/GRE MDT is 1376 and the default value for mLDP/P2MP-TE MDT is 9000 for Multicast VPN.

#### Step 12

**interface all enable**

**Example:**

```
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)#
interface all enable
```

Enables multicast routing and forwarding on all new and existing interfaces.

#### Step 13

**commit**

---

### Specifying the PIM VRF Instance

If you are configuring Protocol Independent Multicast in sparse mode (PIM-SM) in the MVPN, you may also need to configure a rendezvous point (RP). This task specifies the optional PIM VPN instance.

#### SUMMARY STEPS

1. configure
2. `router pim vrf vrf-name address-family {ipv4 | ipv6}`
3. `rp-address ip-address [group-access-list-name] [bidir] [override]`
4. commit

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`router pim vrf vrf-name address-family {ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config)# router pim vrf vrf_A address-family ipv4</code></td>
</tr>
</tbody>
</table>
### Step 3

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `rp-address ip-address [group-access-list-name] [bidir] [override]` | Configures the PIM rendezvous point (RP) address:  
  - `group-access-list-name` = Specifies an access list of groups to be mapped to a given RP.  
  - `bidir` = Specifies a bidirectional RP.  
  - `override` = Specifies that a static RP configuration should override auto-RP and the bootstrap router (BSR). |

**Example:**

```
RP/0/RSP0/CPU0:router(config-pim-vrf_A-ipv4)# rp-address 10.0.0.0
```

### Step 4

<table>
<thead>
<tr>
<th>Command or Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>commit</code></td>
</tr>
</tbody>
</table>

---

### Specifying the IGMP VRF Instance

**SUMMARY STEPS**

1. `configure`
2. `router igmp`
3. `vrf vrf-name`
4. `commit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure</code></td>
<td>Enters IGMP configuration mode.</td>
</tr>
<tr>
<td><code>router igmp</code></td>
<td>Configures a VRF instance.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>Configures a VRF instance.</td>
</tr>
<tr>
<td><code>commit</code></td>
<td>Enters IGMP configuration mode.</td>
</tr>
</tbody>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config)# router igmp
```

```
RP/0/RSP0/CPU0:router(config-igmp)# vrf vrf_B
```

```
RP/0/RSP0/CPU0:router(config-igmp)# vrf vrf_B
```
Configuring the MDT Source per VRF

This optional feature lets you change the default routing mechanism in a multicast VPN network topology, which routes all unicast traffic through a BGP peering loopback configured on a default VRF. Instead, you may configure a loopback that allows you to specify the MDT source using a specific VRF, as opposed to the default VRF. This overrides the current behavior and updates BGP as part of a MDT group. BGP then modifies the source and connector attributes in the MDT SAFI and VPN IPv4 updates.

For VRFs on which the MDT source is not configured, the MDT source for the default VRF is applied. Also, when the MDT source on a VRF is unconfigured, the configuration of the MDT source default VRF takes effect.

In the configuration below, the default VRF does not require explicit reference in Step 5.

### SUMMARY STEPS

1. configure
2. multicast-routing
3. address-family [ ipv4 | ipv6 ]
4. mdt source loopback 0
5. exit
6. vrf 101
7. address-family ipv4
8. mdt source loopback 1
9. Repeat the steps 6 to 8, as many times as needed to create other VRFs.
10. commit
11. show pim vrf all mdt interface

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>multicast-routing</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing RP/0/RSP0/CPU0:router(config-mcast)#</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>address-family [ ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 4</strong> mdt source loopback 0</td>
<td>Configures the interface used to set the MDT source address for MVPN, using the default VRF.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# mdt source loopback 0</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits from the current mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# exit</td>
</tr>
<tr>
<td><strong>Step 6</strong> vrf 101</td>
<td>Enters the IPv4 address-family mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# vrf 101</td>
</tr>
<tr>
<td><strong>Step 7</strong> address-family ipv4</td>
<td>Enters the IPv4 address-family mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-101)# address-family ipv4</td>
</tr>
<tr>
<td><strong>Step 8</strong> mdt source loopback 1</td>
<td>Configures the interface used to set the MDT source address for MVPN.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-101-ipv4)# mdt source loopback 1</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Repeat the steps 6 to 8, as many times as needed to create other VRFs.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# vrf 102 mdt source loopback 2</td>
</tr>
<tr>
<td><strong>Step 10</strong> commit</td>
<td>To verify the MDT source per VRF configuration, use the show pim vrf all mdt interface command.</td>
</tr>
<tr>
<td><strong>Step 11</strong> show pim vrf all mdt interface</td>
<td>To verify the MDT source per VRF configuration, use the show pim vrf all mdt interface command.</td>
</tr>
</tbody>
</table>
Configuring Label Switched Multicast

Deployment of an LSM MLDP-based MVPN involves configuring a default MDT and one or more data MDTs. A static default MDT is established for each multicast domain. The default MDT defines the path used by PE routers to send multicast data and control messages to other PE routers in the multicast domain. A default MDT is created in the core network using a single MP2MP LSP.

An LSP MLDP-based MVPN also supports dynamic creation of the data MDTs for high-bandwidth transmission. For high-rate data sources, a data MDT is created using the P2MP LSPs to off-load the traffic from the default MDT to avoid unnecessary waste of bandwidth to PEs that are not part of the stream. You can configure MLDP MVPN for both the intranet or extranet. This configuration section covers the rosen based MLDP profile. For configuration examples of other MLDP profiles, see Configuring LSM based MLDP: Examples, on page 227.

**Note**

Before configuring MLDP based MVPN, ensure that the MPLS is enabled on the core facing interface. For information in MPLS configuration, see Cisco IOS XR MPLS Configuration Guide. Also, ensure that BGP and any interior gateway protocol (OSPF or ISIS) is enabled on the core router. For more information on BGP and route-policy configuration, see Cisco IOS XR Routing Configuration Guide.

Perform this task to configure label switched multicast:
SUMMARY STEPS

1. configure
2. mpls ldp mldp
3. root
4. vrf vrf_name
5. vpn id vpn-id
6. address-family [ipv4 | ipv6 ] unicast
7. import route-target [xx.yy.nn | as-number:nn | ip-address:nn ]
8. export route-target [xx.yy.nn | as-number:nn | ip-address:nn ]
9. root
10. multicast-routing vrf vrf_name
11. address-family [ipv4 | ipv6 ]
12. mdt default mldp ipv4 root-node
13. mdt data mdt-group-address threshold value
14. root
15. router bgp as-number vrf vrf-name
16. rd route-distinguisher
17. address-family ipv4 mdt
18. address-family vpnv4 unicast
19. root
20. router pim
21. vrf vrf_name
22. address-family [ipv4 | ipv6 ]
23. rpf topology route-policy route_policy_name
24. root
25. route-policy route_policy_name
26. set core-tree tree_type
27. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td></td>
</tr>
<tr>
<td>Step 2 mpls ldp mldp</td>
<td>Enables MPLS MLDP support.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp mldp</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 3</strong> root</td>
<td>Takes the user to the global configuration level.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-ldp-mldp)# root</td>
</tr>
<tr>
<td><strong>Step 4</strong> vrf vrf_name</td>
<td>Configures a VRF instance. The vrf-name argument is the name assigned to a VRF.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config)# vrf vrf1</td>
</tr>
<tr>
<td><strong>Step 5</strong> vpn id vpn-id</td>
<td>Sets or updates a VPN identifier on a VRF.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-vrf)# vpn id 1:1</td>
</tr>
<tr>
<td><strong>Step 6</strong> address-family [ipv4</td>
<td>ipv6 ] unicast</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast</td>
</tr>
<tr>
<td><strong>Step 7</strong> import route-target [xx.yy:nn</td>
<td>as-number:nn</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-vrf-af)# import route-target import 1:1</td>
</tr>
<tr>
<td><strong>Step 8</strong> export route-target [xx.yy:nn</td>
<td>as-number:nn</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-vrf-af)# export route-target export 1:1</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>root</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Takes the user to the global configuration level.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-vrf-af)# root</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>multicast-routing vrf vrf_name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enables multicast routing for the specified VRF.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing vrf vrf1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>address-family [ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters the address-family submode.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-mcast-vrf1)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>mdt default mldp ipv4 root-node</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configures MLDP MDT for a VRF. The root node can be IP address of a loopback or physical interface on any router (source PE, receiver PE or core router) in the provider network. The root node address should be reachable by all the routers in the network. The router from where the signalling occurs functions as the root node. The default MDT must be configured on each PE router to enable the PE routers to receive multicast traffic for this particular MVRF.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-mcast-vrf1-ipv4)# mdt default mldp ipv4 2.2.2.2</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>By default MPLS MLDP is enabled. To disable, use the no mpls ldp mldp command.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>LSPVIF tunnel is created as a result of mdt default mldp root-node command.</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>mdt data mdt-group-address threshold value</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configures the threshold value for data MDT.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-mcast-vrf1-ipv4)# mdt data 239.0.0.0/24 threshold 1000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>root</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Takes the user to the global configuration mode.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-mcast-vrf1-ipv4)# root</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>15</td>
<td>router bgp as-number vrf vrf-name</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config)# router bgp 1 vrf vrf1</td>
</tr>
</tbody>
</table>
| 16    | rd route-distinguisher  | Creates routing and forwarding tables. Specify the route-distinguisher argument to add an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD value in either of these formats:  
  - 16-bit autonomous system number. For example, 101:3.  
  - 32-bit IP address: your 16-bit number. For example, 192.168.122.15:1. |
<p>|       | Example: RP/0/RSP0/CPU0:router(config-bgp-vrf)# rd 1.1.1.1:1 |
| 17    | address-family ipv4 mdt | Configures the BGP MDT address family. |
|       | Example: RP/0/RSP0/CPU0:router(config-bgp-vrf)# address-family ipv4 mdt |
| 18    | address-family vpnv4 unicast | Configures the BGP vpnv4 address family. |
|       | Example: RP/0/RSP0/CPU0:router(config-bgp-af)# address-family vpnv4 unicast |
| 19    | root | Takes the user to the global configuration mode. |
|       | Example: RP/0/RSP0/CPU0:router(config-bgp-af)# root |
| 20    | router pim | Enters the PIM configuration mode. |
|       | Example: RP/0/RSP0/CPU0:router(config)# router pim |
| 21    | vrf vrf_name | Specifies the VRF instance. |
|       | Example: RP/0/RSP0/CPU0:router(config-pim)# vrf vrf1 |</p>
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 22</strong></td>
<td>address-family [ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Enters the address-family submode.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-vrf1)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 23</strong></td>
<td>rpf topology route-policy route_policy_name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Assigns a given routing policy to an RPF topology table.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-vrf1-af)# rpf topology route-policy FOO</td>
<td></td>
</tr>
<tr>
<td><strong>Step 24</strong></td>
<td>root</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Takes the user to the global configuration mode.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-vrf1-af)# root</td>
<td></td>
</tr>
<tr>
<td><strong>Step 25</strong></td>
<td>route-policy route_policy_name</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Configures the route policy for a profile. For more information about configuring route policy, see <em>Cisco IOS XR Routing Configuration Guide</em>.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# route-policy FOO</td>
<td></td>
</tr>
<tr>
<td><strong>Step 26</strong></td>
<td>set core-tree tree_type</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Specifies the MDT type for the route policy.</td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-rpl)# set core-tree mldp-rosen</td>
<td></td>
</tr>
<tr>
<td><strong>Step 27</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

### Verification of LSM mLDP based MVPN Configuration

Use these commands to verify the LSM mLDP based MVPN intranet configuration:

- To check the MLDP neighbors, use the `show mpls mldp neighbors` command:

```plaintext
Router# show mpls mldp neighbors
mLDP neighbor database
MLDP peer ID : 1.0.0.1:0, uptime 15:36:30 Up,
Capabilities  : GR, Typed Wildcard FEC, P2MP, MP2MP, MBB
Target Adj    : No
Upstream count : 0
Branch count  : 0
LDP GR        : Enabled
```
To check the PIM neighbors, use the `show pim vrf vrf-name neighbor` command:

```
Router# show pim vrf A1_MIPMSI neighbor
PIM neighbors in VRF A1_MIPMSI

Neighbor Address        Interface   Uptime      Expires  DR pri s
101.2.2.101*            Loopback2  15:54:43     00:00:02  1 (DR) BP
```
To check the multicast routes for a given VRF, use the `show mrib vrf vrf_name route` command:

```bash
Router# show mrib vrf A1_MIPMSI route
```

**IP Multicast Routing Information Base**

Entry flags:  
L - Domain-Local Source, E - External Source to the Domain,  
C - Directly-Connected Check, S - Signal, IA - Inherit Accept,  
IF - Inherit From, D - Drop, MA - MDT Address, ME - MDT Encap,  
MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle  
CD - Conditional Decap, MPLS - MPLS Decap, MF - MPLS Encap, EX - Extranet  
MoTE - MoFRR Enabled, MoFS - MoFRR State  
Interface flags:  
F - Forward, A - Accept, IC - Internal Copy,  
NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,  
II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,  
LD - Local Disinterest, DI - Decapsulation Interface  
EI - Encapsulation Interface, MI - MDT Interface, LVIF - MPLS Encap,  
EX - Extranet, A2 - Secondary Accept

```
(*,224.0.0.0/24) Flags: D  
Op: 15:57:19
```

```
(*,224.0.1.39) Flags: S  
Up: 15:57:19
```

```
(*,224.0.1.40) Flags: S  
Up: 15:57:19
```

**Outgoing Interface List**

Serial0/5/0/0/1 Flags: II LI, Up: 15:57:12

```
(*,225.0.0.0/19) RPF nbr: 101.2.2.101 Flags: L C  
Op: 15:57:19
```

**Outgoing Interface List**

Decaps tunnel98 Flags: NS DI, Up: 15:57:10

```
(*,225.0.32.0/19) RPF nbr: 102.0.0.102 Flags: C  
Up: 15:57:19
```

```
(*,225.0.32.0) RPF nbr: 102.0.0.102 Flags: C  
Op: 04:08:30
```

**Incoming Interface List**

LmdtA1/MIPMSI Flags: A LMI, Up: 04:08:30

**Outgoing Interface List**

Serial0/2/0/1/1.16 Flags: FC NS, Up: 04:08:30

```
(*,225.0.32.2) RPF nbr: 102.0.0.102 Flags: C  
Op: 04:08:30
```

**Incoming Interface List**

LmdtA1/MIPMSI Flags: A LMI, Up: 04:08:30

**Outgoing Interface List**

Serial0/2/0/1/1.16 Flags: FC NS, Up: 04:08:30

```
(*,225.0.32.3) RPF nbr: 102.0.0.102 Flags: C  
Op: 04:08:30
```

**Incoming Interface List**

LmdtA1/MIPMSI Flags: A LMI, Up: 04:08:30
Configuring MVPN Static P2MP-TE

Perform these steps to configure the multicast VPN for static point-to-multipoint (P2MP) traffic engineering (TE).

Configuring MVPN P2MP on Ingress PE

Perform this task to configure MVPN P2MP on Ingress PE.

SUMMARY STEPS

1. configure
2. multicast-routing
3. address-family {ipv4|ipv6}
4. mdt source type interface-path-id
5. interface all enable
6. vrf vrf-name
7. address-family {ipv4 | ipv6}
8. bgp auto-discovery rsvpte
9. mdt static p2mp-te tunnel-mte value
10. interface all enable
11. router igmp
12. vrf name
13. interface type interface-path-id
14. static-group ip_group_address source-address
15. commit
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>multicast-routing</td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>mdt source type interface-path-id</td>
<td>Specifies the MDT source address.</td>
</tr>
<tr>
<td></td>
<td>Note: The MDT source interface name should be the same as the one used for BGP peerings.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# mdt source Loopback 0</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>interface all enable</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces. You can also enable individual interfaces.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>vrf vrf-name</td>
<td>Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# vrf vrf1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-vrf1)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>bgp auto-discovery rsvpte</td>
<td>Enables the RSVP-TE I-PMSI core tree.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-vrf1-ipv4)# bgp auto-discovery rsvp-te</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>9</td>
<td>mdt static p2mp-te tunnel-mte value</td>
<td>Specifies the static p2mp-te mpls traffic engineering P2MP tunnel interface.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# mdt static p2mp-te tunnel-mte 1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>interface all enable</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces. You can also enable individual interfaces.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>router igmp</td>
<td>Configures router igmp and enters the igmp configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config)# router igmp</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>vrf name</td>
<td>Sets conditions for the access list to recognize the source as part of the specified access list set, in which each ACL describes a set of SSM groups to be mapped.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-igmp)# vrf vrf1</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>interface type interface-path-id</td>
<td>Configures the MPLS Traffic Engineering P2MP tunnel interface.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-igmp)# interface tunnel-mte1</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>static-group ip_group_address source-address</td>
<td>Configures the IGMP static multicast group.</td>
</tr>
<tr>
<td></td>
<td>Example: RP/0/RSP0/CPU0:router(config-igmp-default-if)# static-group 232.1.1.1 192.1.1.2</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring MVPN P2MP BGP

Perform this task to configure MVPN P2MP BGP.
### SUMMARY STEPS

1. configure
2. router bgp 100
3. bgp router-id ip_address
4. address-family {ipv4 | ipv6} unicast
5. address-family {vpnv4 | vpnv6} unicast
6. address-family {ipv4 | ipv6} mvpn
7. neighbor address
8. remote-as 2-byte AS number
9. update-source interface type interface-path-id
10. address-family {ipv4 | ipv6} unicast
11. address-family {vpnv4 | vpnv6} unicast
12. address-family {ipv4 | ipv6} mvpn
13. vrf name
14. rd x.y format
15. bgp router-id ip_address
16. address-family {ipv4 | ipv6} unicast
17. redistribute connected
18. address-family {ipv4 | ipv6} mvpn
19. commit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>router bgp 100</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# router bgp 100</td>
<td>Configures the BGP routing process.</td>
</tr>
<tr>
<td>3</td>
<td>bgp router-id ip_address</td>
<td>Configures the router-id for the BGP protocol.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 12.33.42.34</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>address-family {ipv4</td>
<td>ipv6} unicast</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-bgp)# address-family</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>ipv4 unicast</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 5**

address-family {vpnv4 | vpnv6} unicast  
*Example:*  
RP/0/RSP0/CPU0:router(config-bgp)# address-family vpng4 unicast

Configures vpng4 address-family for unicast and enters the address family command mode.

**Step 6**

address-family {ipv4 | ipv6} mvpn  
*Example:*  
RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 mvpn

Configures ipv4 address-family for mvpn and enters the address family command mode.

**Step 7**

neighbor *address*  
*Example:*  
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 1.3.45.6

Specifies a neighbor router.

**Step 8**

remote-as 2-byte *AS number*  
*Example:*  
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 100

Set remote AS with the specified 2-byte AS number.

**Step 9**

update-source interface type interface-path-id  
*Example:*  
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 1

Set remote AS with the specified 2-byte AS number.

**Step 10**

address-family {ipv4 | ipv6} unicast  
*Example:*  
RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast

Configures ipv4 address-family for unicast and enters the address family command mode.

**Step 11**

address-family {vpnv4 | vpnv6} unicast  
*Example:*  
RP/0/RSP0/CPU0:router(config-bgp)# address-family vpng4 unicast

Configures vpng4 address-family for unicast and enters the address family command mode.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>`address-family {ipv4</td>
<td>ipv6} mvpn`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 mvpn</code></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td><code>vrf name</code></td>
<td>Configures the VRF.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# vrf vrf1</code></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td><code>rd x.y format</code></td>
<td>Configures the route distinguisher.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-vrf)# rd 1:1</code></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><code>bgp router-id ip_address</code></td>
<td>Configures the router-id for the BGP protocol.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 12.33.42.34</code></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>`address-family {ipv4</td>
<td>ipv6} unicast`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast</code></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td><code>redistribute connected</code></td>
<td>Redistributes information from another routing protocol through connected routes.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-af)# redistribute connected</code></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>`address-family {ipv4</td>
<td>ipv6} mvpn`</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 mvpn</code></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td><code>commit</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring MVPN P2MP on Egress PE

Perform this task to configure MVPN P2MP on egress PE.

### SUMMARY STEPS

1. `configure`
2. `multicast-routing`
3. `address-family {ipv4|ipv6}`
4. `mdt source type interface-path-id`
5. `interface all enable`
6. `vrf vrf-name`
7. `address-family {ipv4 | ipv6}`
8. `core-tree-protocol rsvp-te group-list name`
9. `interface all enable`
10. `ipv4 access-list acl-name`
11. `[sequence-number] permit ipv4 host source_address host [destination_address]`
12. `[sequence-number] permit ipv4 any host destination_address`
13. `commit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>multicast-routing</code></td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing</td>
</tr>
<tr>
<td>Step 3</td>
<td>`address-family {ipv4</td>
<td>ipv6}`</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>mdt source type interface-path-id</code></td>
<td>Specifies the MDT source address.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# mdt source Loopback 1</td>
</tr>
<tr>
<td>Note</td>
<td>The MDT source interface name should be the same as the one used for BGP peerings.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>interface all enable</strong></td>
<td>Enables multicast routing and forwarding on all new and existing interfaces. You can also enable individual interfaces.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td><strong>vrf vrf-name</strong></td>
<td>Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# vrf vrf1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>**address-family {ipv4</td>
<td>ipv6}**</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-vrf1)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>core-tree-protocol rsvp-te group-list name</strong></td>
<td>Configures RSVP-TE as the core-tree-protocol and enters the core-tree-protocol configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-vrf1-ipv4)# core-tree-protocol rsvp-te group-list mvpn_acl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>interface all enable</strong></td>
<td>Enables multicast routing and forwarding on all new and existing interfaces. You can also enable individual interfaces.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>ipv4 access-list acl-name</strong></td>
<td>Enters IPv4 ACL configuration submode and creates a name for an IPv4 access list.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# ipv4 access-list mvpn_acl</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td><strong>[sequence-number] permit ipv4 host source_address host [destination_address]</strong></td>
<td>Sets conditions for the access list to recognize the source as part of the specified access list set.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit 1 host 232.1.1.2 any</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring MVPN InterAS Options

Perform these steps to configure the various MVPN InterAS options:

#### Configuring a PE Router for MVPN InterAS Option B or C

Perform this step to configure a PE router for MVPN InterAS option B or C:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 12: <code>[sequence-number] permit ipv4 any host destination_address</code></td>
<td>Sets conditions for the access list to recognize the source as part of the specified access list set.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-ipv4-acl)# 20 permit ipv4 any host 232.1.1.2</td>
<td></td>
</tr>
<tr>
<td>Step 13: <code>commit</code></td>
<td></td>
</tr>
</tbody>
</table>
SUMMARY STEPS

1. configure
2. vrf vpn1
3. address-family ipv4 unicast
4. import route-target 2-byte AS number
5. export route-target 2-byte AS number
6. router bgp 2-byte AS number
7. bgp router-id ipv4 address
8. address-family ipv4 unicast
9. allocate-label all
10. address-family vpnv4 unicast
11. address-family ipv4 mvpn
12. neighbor neighbor_address
13. remote-as 2-byte AS number
14. update-source Loopback 0-655335
15. address-family ipv4 labeled-unicast
16. address-family vpnv4 unicast
17. inter-as install
18. address-family ipv4 mvpn
19. vrf vpn1
20. rd 2-byte AS number
21. address-family ipv4 unicast
22. route-target download
23. address-family ipv4 mvpn
24. inter-as install
25. mpls ldp
26. router-id ip address
27. mldp recursive-fec
28. interface type interface-path-id
29. multicast-routing
30. address-family ipv4
31. mdt source type interface-path-id
32. interface all enable
33. vrf vpn1
34. address-family ipv4
35. bgp auto-discovery mldp inter-as
36. mdt partitioned mldp ipv4 mp2mp
37. interface all enable
38. router pim
39. vrf vrf1
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Configure the vrf and enters the vrf configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> vrf vpn1</td>
<td>Configures the vrf and enters the vrf configuration mode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# vrf vpn1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> address-family ipv4 unicast</td>
<td>Configures the ipv4 address-family for a unicast topology and enters the ipv4 address-family submode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> import route-target 2-byte AS number</td>
<td>Specifies the 2-byte AS number for the import route target extended communities.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-vrf-af)# import route-target 20:1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> export route-target 2-byte AS number</td>
<td>Specifies the 2-byte AS number for the export route target extended communities.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-vrf-af)# export route-target 10:1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> router bgp 2-byte AS number</td>
<td>Configures the router bgp and enters the router bgp configuration mode.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# router bgp 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> bgp router-id ipv4 address</td>
<td>Configures the bgp router id with the ipv4 address.</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 10.10.10.1</td>
<td></td>
</tr>
</tbody>
</table>

**Note** Steps 1 to 7 are common for both Option B and C.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 8** | **address-family ipv4 unicast**  
**Example:**  
RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast  
Configures the ipv4 address-family with the unicast topology. |
| **Step 9** | **allocate-label all**  
**Example:**  
RP/0/RSP0/CPU0:router(config-bgp)# allocate-label all  
Allocates label for all prefixes.  
**Note** Steps 8 and 9 are part of the Option C configuration. |
| **Step 10** | **address-family vpnv4 unicast**  
**Example:**  
RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv4 unicast  
Configures the vpnv4 address-family with the unicast topology. |
| **Step 11** | **address-family ipv4 mvpn**  
**Example:**  
RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 mvpn  
Configures the ipv4 address-family with the mvpn. |
| **Step 12** | **neighbor neighbor_address**  
**Example:**  
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 10.10.10.02  
Specifies and configures a neighbor router with the neighbor address. |
| **Step 13** | **remote-as 2-byte AS number**  
**Example:**  
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 100  
Sets remote AS with the mentioned 2-byte AS number. |
| **Step 14** | **update-source Loopback 0-655335**  
**Example:**  
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 0  
Specifies the source of routing updates using the Loopback interface.  
**Note** Steps 10 to 14 are common to both Option B and C. |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>address-family ipv4 labeled-unicast</td>
<td>Configures the ipv4 address-family with the labeled unicast topology. <strong>Note</strong> Step 15 is only performed for Option C configuration.</td>
</tr>
<tr>
<td>16</td>
<td>address-family vpnv4 unicast</td>
<td>Configures the vpnv4 address-family with the unicast topology. <strong>Note</strong> Step 16 is common to both Option B and C.</td>
</tr>
<tr>
<td>17</td>
<td>inter-as install</td>
<td>Installs Inter-AS option. <strong>Note</strong> Step 17 is only for Option B configuration.</td>
</tr>
<tr>
<td>18</td>
<td>address-family ipv4 mvpn</td>
<td>Configures the ipv4 address-family with the mvpn.</td>
</tr>
<tr>
<td>19</td>
<td>vrf vpn1</td>
<td>Configures the vrf and enters the vrf configuration mode.</td>
</tr>
<tr>
<td>20</td>
<td>rd 2-byte AS number</td>
<td>Configures the route distinguisher with a 2-byte AS number.</td>
</tr>
<tr>
<td>21</td>
<td>address-family ipv4 unicast</td>
<td>Configures the ipv4 address-family for a unicast topology and enters the ipv4 address-family submode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Step 22 route-target download</td>
<td>Installs and configures the route-targets in RIB.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# route-target download</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 23 address-family ipv4 mvpn</td>
<td>Configures the ipv4 address-family with the mvpn.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp-vrf)# address-family ipv4 mvpn</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>Steps 18 to 23 are common to both Option B and C.</td>
<td></td>
</tr>
<tr>
<td>Step 24 inter-as install</td>
<td>Installs Inter-AS option.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr)# inter-as install</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>Step 24 is only for Option C configuration.</td>
<td></td>
</tr>
<tr>
<td>Step 25 mpls ldp</td>
<td>Configures the MPLS label distribution protocol (ldp).</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td>Steps 25 till 44 are common to both Option B and C.</td>
<td></td>
</tr>
<tr>
<td>Step 26 router-id ip address</td>
<td>Configures the router id with the ip address.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp)# router-id 10.10.10.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 27 mldp recursive-fec</td>
<td>Configures the mLDP recursive FEC support.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp)# mldp recursive-fec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 28 interface type interface-path-id</td>
<td>Configures the GigabitEthernet/IEEE 802.3 interface(s).</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-ldp)# interface GigabitEthernet 0/1/0/0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 29</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>multicast-routing</strong></td>
<td>Enables IP Multicast forwarding and enters the multicast routing configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# multicast-routing</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 30</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address-family ipv4</strong></td>
<td>Configures the ipv4 address-family and enters ipv4 address-family submode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 31</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mdt source type interface-path-id</strong></td>
<td>Configures mvpn and specifies the interface used to set MDT source address.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# mdt source Loopback 0</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 32</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface all enable</strong></td>
<td>Enables multicast routing and forwarding on all new and existing interfaces. You can also enable individual interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 33</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vrf vpn1</strong></td>
<td>Configures the vrf and enters the vrf configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-mcast)# vrf vpn1</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 34</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address-family ipv4</strong></td>
<td>Configures the ipv4 address-family and enters the ipv4 address-family submode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-mcast-vpn1)# address-family ipv4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 35</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bgp auto-discovery mldp inter-as</strong></td>
<td>enables BGP MVPN auto-discovery.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-mcast-vpn1-ipv4)# bgp auto-discovery mldp inter-as</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 36</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>mdt partitioned mldp ipv4 mp2mp</strong></td>
<td>Enables MLDP MP2MP signaled partitioned distribution tree for ipv4 core.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-mcast-vpn1-ipv4)#</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>mdt partitioned mldp ipv4 mp2mp</td>
<td>Note</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 37</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface all enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-mcast-vpn1-ipv4)#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>interface all enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 38</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>router pim</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# router pim</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 39</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vrf vrf1</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim)# vrf vrf1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 40</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>address-family ipv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-vrf1)# address-family</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ipv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 41</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rpf topology route-policy policy_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-pim-vrf1-ipv4)#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rpf topology route-policy MSPMSI_MP2MP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 42</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>route-policy policy_name</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# route-policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSPMSI_MP2MP</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 43</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>set core-tree mldp-partitioned-mp2mp</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-rpl)# set core-tree</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring ASBR Router for MVPN InterAS Option B or C

Perform this step to configure ASBR router for MVPN InterAS Option B or C:

**Before You Begin**

Perform these steps prior to starting the Configuring ASBR Router for MVPN InterAS Option B or C:

```plaintext
prefix-set IGP_leaks
  10.10.10.1/32,
  10.10.10.2/32,
  10.10.10.3/32
end-set

route-policy IGP_INTER_AS_C_OUT
  if destination in IGP_leaks then
    pass
  else
    drop
  endif
end-policy
```

---

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>mldp-partitioned-mp2mp</td>
<td></td>
</tr>
</tbody>
</table>

Step 44 commit
SUMMARY STEPS

1. configure
2. router static
3. address-family ipv4 unicast destination prefix interface-type interface-path-id
4. router bgp 2-byte AS number
5. bgp router-id ipv4 address
6. address-family vpnv4 unicast
7. retain route-target all
8. address-family ipv4 mvpn
9. retain route-target all
10. address-family ipv4 unicast
11. redistribute ospf router_tag
12. route-policy policy_name
13. allocate-label all
14. neighbor neighbor_address
15. remote-as 2-byte AS number
16. update-source interface 0-65535
17. address-family vpnv4 unicast
18. address-family ipv4 labeled-unicast
19. route-policy policy_name in
20. route-policy policy_name out
21. neighbor neighbor_address
22. remote-as 2-byte AS number
23. update-source Loopback 0-65535
24. address-family vpnv4 unicast
25. address-family ipv4 labeled-unicast
26. next-hop-self
27. address-family ipv4 mvpn
28. next-hop-self
29. mpls ldp
30. router-id ip address
31. mldp recursive-fec
32. interface type interface-path-id
33. discovery transport-address ip_address
34. interface type interface-path-id
35. commit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>router static</td>
</tr>
<tr>
<td>Example:</td>
<td>router static</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>address-family ipv4 unicast destination prefix interface-type interface-path-id</td>
</tr>
<tr>
<td>Example:</td>
<td>address-family ipv4 unicast 3.3.3.3/32 GigabitEthernet 0/1/0/1</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>router bgp 2-byte AS number</td>
</tr>
<tr>
<td>Example:</td>
<td>router bgp 2-byte AS number</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>bgp router-id ipv4 address</td>
</tr>
<tr>
<td>Example:</td>
<td>bgp router-id ipv4 address</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>address-family vpv4 unicast</td>
</tr>
<tr>
<td>Example:</td>
<td>address-family vpv4 unicast</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>retain route-target all</td>
</tr>
<tr>
<td>Example:</td>
<td>retain route-target all</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>address-family ipv4 mvpn</td>
</tr>
</tbody>
</table>
| Example:          | address-family ipv4 mvpn | RP/0/RSP0/CPU0:router(config-bgp)# address-family
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 mvpn</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> retain route-target all</td>
<td>Accepts or retains the received updates containing at least one route target.</td>
<td>Steps 6 to 9 are only for Option B Configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp-af)# retain route-target all</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> address-family ipv4 unicast</td>
<td>Configures the ipv4 address-family for a unicast topology and enters the ipv4 address-family submode.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> redistribute ospf router_tag</td>
<td>Redistributes information from another routing protocol.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp-af)# redistribute ospf 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> route-policy policy_name</td>
<td>Configures the route-policy to select RPF topology.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config)# route-policy IGP_INTER_AS_C_OUT</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 13</strong> allocate-label all</td>
<td>Allocates label for all prefixes.</td>
<td>Steps 10 and 13 are part of the Option C configuration.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp)# allocate-label all</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 14</strong> neighbor neighbor_address</td>
<td>Specifies and configures a neighbor router with the neighbor address.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp)# neighbor 10.10.10.02</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 15</strong> remote-as 2-byte AS number</td>
<td>Sets remote AS with the mentioned 2-byte AS number.</td>
<td>Steps 14 and 15 are common to both Option B and C.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 100</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>16</td>
<td><code>update-source interface 0-65535</code></td>
<td>Specifies the source of routing updates using the GigabitEthernet interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source GigabitEthernet 0/1/0/1</td>
<td></td>
</tr>
</tbody>
</table>
| 17   | `address-family vpnv4 unicast` | Configures the vpnv4 address-family with the unicast topology.  
|     | Note: Steps 16 and 17 are for Option B configuration. |         |
|     | Example:          |         |
|     | RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast |         |
| 18   | `address-family ipv4 labeled-unicast` | Configures the ipv4 address-family with the labeled unicast topology.  
|     | Note: Step 18 is only performed for Option C configuration. |         |
|     | Example:          |         |
|     | RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast |         |
| 19   | `route-policy policy_name in` | Applies route-policy to inbound routes. |
|     | Example:          |         |
|     | RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in |         |
| 20   | `route-policy policy_name out` | Applies route-policy to outbound routes.  
<p>|     | Note: Steps 19 and 20 are common to both Option B and C. |         |
|     | Example:          |         |
|     | RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out |         |
| 21   | <code>neighbor neighbor_address</code> | Specifies and configures a neighbor router with the neighbor address. |
|     | Example:          |         |
|     | RP/0/RSP0/CPU0:router(config-bgp)# neighbor 10.10.10.02 |         |
| 22   | <code>remote-as 2-byte AS number</code> | Sets remote AS with the mentioned 2-byte AS number. |
|     | Example:          |         |
|     | RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 100 |         |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 23</td>
<td>update-source Loopback 0-65535</td>
<td>Specifies the source of routing updates using the Loopback interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 0/1/0/1</td>
<td></td>
</tr>
<tr>
<td>Step 24</td>
<td>address-family vvpn4 unicast</td>
<td>Configures the vvpn4 address-family with the unicast topology.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-bgp)# address-family vvpn4 unicast</td>
<td></td>
</tr>
<tr>
<td>Step 25</td>
<td>address-family ipv4 labeled-unicast</td>
<td>Configures the ipv4 address-family with the labeled unicast topology.</td>
</tr>
<tr>
<td>Note:</td>
<td>Step 25 is only performed for Option C configuration.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast</td>
<td></td>
</tr>
<tr>
<td>Step 26</td>
<td>next-hop-self</td>
<td>Disables the next hop calculation for this neighbor.</td>
</tr>
<tr>
<td>Note:</td>
<td>Steps 21 to 26 are common to both Option B and C, except 25 that is only applicable for Option C.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# next-hop-self</td>
<td></td>
</tr>
<tr>
<td>Step 27</td>
<td>address-family ipv4 mvpn</td>
<td>Configures the ipv4 address-family with the mvpn.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 mvpn</td>
<td></td>
</tr>
<tr>
<td>Step 28</td>
<td>next-hop-self</td>
<td>Disables the next hop calculation for this neighbor.</td>
</tr>
<tr>
<td>Note:</td>
<td>Steps 25 and 26 are applicable only for Option B configuration.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# next-hop-self</td>
<td></td>
</tr>
<tr>
<td>Step 29</td>
<td>mpls ldp</td>
<td>Configures the MPLS label distribution protocol (ldp).</td>
</tr>
<tr>
<td>Note:</td>
<td>Steps 27 to 33 are common to both Option B and C.</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# mpls ldp</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 30</strong></td>
<td>Configure the router id with the ip address.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# router-id 10.10.10.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 31</strong></td>
<td>Configure the mLDP recursive FEC support.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# mldp recursive-fec</td>
<td></td>
</tr>
<tr>
<td><strong>Step 32</strong></td>
<td>Configures the GigabitEthernet/IEEE 802.3 interface(s).</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# interface GigabitEthernet 0/1/0/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 33</strong></td>
<td>Configures interface LDP discovery parameters by specifying the interface LDP transport address.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-ldp-if)# discovery transport-address 3.3.3.2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 34</strong></td>
<td>Configures the GigabitEthernet/IEEE 802.3 interface(s).</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-ldp)# interface GigabitEthernet 0/1/0/1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 35</strong></td>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring RR for MVPN InterAS Option C**

Perform this step to configure RR for MVPN InterAS Option C:
SUMMARY STEPS

1. configure
2. router bgp 2-byte AS number
3. bgp router-id ipv4 address
4. address-family ipv4 unicast
5. allocate-label all
6. address-family vpnv4 unicast
7. address-family ipv4 mvpn
8. neighbor neighbor_address
9. remote-as 2-byte AS number
10. update-source Loopback 0-655335
11. address-family ipv4 labeled-unicast
12. route-reflector-client
13. address-family vpnv4 unicast
14. route-reflector-client
15. address-family ipv4 mvpn
16. route-reflector-client
17. neighbor neighbor_address
18. remote-as 2-byte AS number
19. update-source Loopback 0-655335
20. address-family ipv4 labeled-unicast
21. route-reflector-client
22. neighbor neighbor_address
23. remote-as 2-byte AS number
24. update-source Loopback 0-655335
25. address-family vpnv4 unicast
26. route-policy policy_name in
27. route-policy policy_name out
28. next-hop-unchanged
29. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>router bgp 2-byte AS number</td>
<td>Configures the router bgp and enters the router bgp configuration mode.</td>
</tr>
</tbody>
</table>

Example:

RP/0/RSP0/CPU0:router(config)# router bgp 100
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td><code>bgp router-id ipv4 address</code></td>
<td>Configures the bgp router id with the ipv4 address.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 10.10.10.1</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>address-family ipv4 unicast</code></td>
<td>Configures the ipv4 address-family for a unicast topology and enters the ipv4 address-family submode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>allocate-label all</code></td>
<td>Allocates label for all prefixes.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-af)# allocate-label all</code></td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td><code>address-family vpnv4 unicast</code></td>
<td>Configures the vpnv4 address-family with the unicast topology.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv4 unicast</code></td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td><code>address-family ipv4 mvpn</code></td>
<td>Configures the ipv4 address-family with the mvpn.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 mvpn</code></td>
<td></td>
</tr>
<tr>
<td>Step 8</td>
<td><code>neighbor neighbor_address</code></td>
<td>Specifies and configures a neighbor router with the neighbor address.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# neighbor 10.10.10.1</code></td>
<td></td>
</tr>
<tr>
<td>Step 9</td>
<td><code>remote-as 2-byte AS number</code></td>
<td>Sets remote AS with the mentioned 2-byte AS number.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 100</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Step 10</td>
<td><code>update-source Loopback 0-65535</code></td>
<td>Specifies the source of routing updates using the Loopback interface.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 0</code></td>
<td></td>
</tr>
<tr>
<td>Step 11</td>
<td><code>address-family ipv4 labeled-unicast</code></td>
<td>Configures the ipv4 address-family with the labeled unicast topology.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast</code></td>
<td></td>
</tr>
<tr>
<td>Step 12</td>
<td><code>route-reflector-client</code></td>
<td>Configures a neighbor as route reflector client.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-nbr)# route-reflector-client</code></td>
<td></td>
</tr>
<tr>
<td>Step 13</td>
<td><code>address-family vpnv4 unicast</code></td>
<td>Configures the vpnv4 address-family with the unicast topology.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv4 unicast</code></td>
<td></td>
</tr>
<tr>
<td>Step 14</td>
<td><code>route-reflector-client</code></td>
<td>Configures a neighbor as route reflector client.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client</code></td>
<td></td>
</tr>
<tr>
<td>Step 15</td>
<td><code>address-family ipv4 mvpn</code></td>
<td>Configures the ipv4 address-family with the mvpn.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 mvpn</code></td>
<td></td>
</tr>
<tr>
<td>Step 16</td>
<td><code>route-reflector-client</code></td>
<td>Configures a neighbor as route reflector client.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client</code></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>
| **Step 17**
neighbor neighbor_address | Specifies and configures a neighbor router with the neighbor address. |
| Example:
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 10.10.10.2 | |
| **Step 18**
remote-as 2-byte AS number | Sets remote AS with the mentioned 2-byte AS number. |
| Example:
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 100 | |
| **Step 19**
update-source Loopback 0-65535 | Specifies the source of routing updates using the Loopback interface. |
| Example:
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 0 | |
| **Step 20**
address-family ipv4 labeled-unicast | Configures the ipv4 address-family with the labeled unicast topology. |
| Example:
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast | |
| **Step 21**
route-reflector-client | Configures a neighbor as route reflector client. |
| Example:
RP/0/RSP0/CPU0:router(config-bgp-nbr)# route-reflector-client | |
| **Step 22**
neighbor neighbor_address | Specifies and configures a neighbor router with the neighbor address. |
| Example:
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 20.20.20.3 | |
| **Step 23**
remote-as 2-byte AS number | Sets remote AS with the mentioned 2-byte AS number. |
| Example:
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 200 | |
### Configuring Multitopology Routing

This set of procedures configures multitopology routing, which is used by PIM for reverse-path forwarding (RPF) path selection.

- "Configuring a Global Topology and Associating It with an Interface" (required)
  For information, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.
- "Enabling an IS-IS Topology" (required)
  For information, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 24</strong></td>
<td>update-source Loopback 0-65535</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source Loopback 0</td>
</tr>
<tr>
<td></td>
<td>Specifies the source of routing updates using the Loopback interface.</td>
</tr>
<tr>
<td><strong>Step 25</strong></td>
<td>address-family vpnv4 unicast</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast</td>
</tr>
<tr>
<td></td>
<td>Configures the vpnv4 address-family with the unicast topology.</td>
</tr>
<tr>
<td><strong>Step 26</strong></td>
<td>route-policy policy_name in</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in</td>
</tr>
<tr>
<td></td>
<td>Applies route-policy to inbound routes.</td>
</tr>
<tr>
<td><strong>Step 27</strong></td>
<td>route-policy policy_name out</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out</td>
</tr>
<tr>
<td></td>
<td>Applies route-policy to outbound routes.</td>
</tr>
<tr>
<td><strong>Step 28</strong></td>
<td>next-hop-unchanged</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# next-hop-unchanged</td>
</tr>
<tr>
<td></td>
<td>Indicates that the next hop should be kept as is and not overwritten, before advertising to eBGP peers.</td>
</tr>
<tr>
<td><strong>Step 29</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>
Restrictions for Configuring Multitopology Routing

- Only the default VRF is currently supported in a multitopology solution.
- Only protocol-independent multicast (PIM) and intermediate system-intermediate system (IS-IS) routing protocols are currently supported.
- Topology selection is restricted solely to (S, G) route sources for both SM and SSM. Static and IS-IS are the only interior gateway protocols (IGPs) that support multitopology deployment.

For non-(S, G) route sources like a rendezvous point or bootstrap router (BSR), or when a route policy is not configured, the current policy default remains in effect. In other words, either a unicast-default or multicast-default table is selected for all sources based on any of the following configurations:

- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)
- Multiprotocol Border Gateway Protocol (MBGP)

Note

Although both multicast and unicast keywords are available when using the address-family \{ipv4 | ipv6\} command in routing policy language (RPL), only topologies under multicast SAFI can be configured globally.

Information About Multitopology Routing

Configuring multitopology networks requires the following tasks:

- "Configuring a Global Topology and Associating It with an Interface" (required)
  For information, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.
- "Enabling an IS-IS Topology" (required)
  For information, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.
- "Placing an Interface in a Topology in IS-IS" (required)
  For information, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.
- "Configuring a Routing Policy" (required)
  For information, see Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.
Configuring an RPF Topology in PIM

**SUMMARY STEPS**

1. configure
2. router pim address-family {ipv4 | ipv6}
3. rpf topology route-policy policy-name
4. exit
5. multicast-routing address-family {ipv4 | ipv6}
6. interface all enable
7. commit
8. show pim [vrf vrf-name] [ipv4 | ipv6] [ {unicast | multicast | safi-all} topology {table-name | all}] rpf [ip-address | hash | summary | route-policy]

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enters PIM address-family configuration submode for the IP prefix you select.</td>
</tr>
<tr>
<td>Step 2</td>
<td>router pim address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)#</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-pim-default-ipv4)#</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>rpf topology route-policy policy-name</td>
<td>Assigns a given routing policy to an RPF topology table.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# rpf topology route-policy mtpolicy</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Exits pim address-family configuration submode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-pim-default-ipv6)# exit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)#</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>multicast-routing address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing address-family ipv4</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> interface all enable</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-mcast-default- ipv4))# interface all enable</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> commit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> show pim [vrf vrf-name] [ipv4</td>
<td>ipv6] [ {unicast</td>
<td>multicast</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# show pim vrf mtt rpf ipv4 multicast topology all rpf</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Configuring MVPN Extranet Routing

To be able to import unicast routes from source VRFs to receiver VRFs, the import route targets of receiver VRFs must match the export route targets of a source VRF. Also, all VRFs on the PEs where the extranet source-receiver switchover takes place should be added to the BGP router configuration on those PEs.

Configuring MVPN extranet routing consists of these mandatory and optional tasks, which should be performed in the sequence shown:

- “Configuring a Routing Policy” (required only if performing the following task)

  For information, see *Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide*.

For examples of an end-to-end configuration of each of the two available MVPN extranet topology solutions, see Configuring MVPN Extranet Routing: Example, on page 207.

### Prerequisites for MVPN Extranet Routing

- PIM-SM and PIM-SSM are supported. You must configure the multicast group range in the source and receiver VRFs with a matching PIM mode.
- Because only static RP configuration is currently supported for a given multicast group range, both source and receiver MVRFs must be configured with the same RP.
- In the IPv6 Connectivity over MVPN topology model, the data MDT encapsulation range should be large enough to accommodate extranet streams without any aggregation. This prevents extranet traffic, flowing to multiple VRFs, from being carried into only one data MDT.
- Data MDT configuration is required on only the Source VRF and Source PE Router.
Restrictions for MVPN Extranet Routing

- PIM-DM and PIM-BIDIR are not supported.
- Cisco IOS XR Software software supports only IPv4 extranet multicast routing over IPv4 core multicast routing.
- Any PE can be configured as an RP except a PE in the "Receiver VRF on the Source PE Router" model where the extranet switchover occurs, and where the source VRF has no interfaces. This is because the source VRF must have some physical interface to signal the data packets being received from the first hop.
- Cisco IOS XR Software currently supports only one encapsulation of VRF traffic on an extranet. This means that only one encapsulation interface (or MDT) is allowed in the outgoing forwarding interface list of the multicast route. If, for a given stream, there are multiple receiver VRFs joining the same source VRF, only the first receiver VRF receives traffic; other receiver VRF joins are discarded.

Note: This limitation applies only to IPv6 Connectivity over MVPN topology model.

Configuring VPN Route Targets

This procedure demonstrates how to configure a VPN route target for each topology.

Note: Route targets should be configured so that the receiver VRF has unicast reachability to prefixes in the source VRF. These configuration steps can be skipped if prefixes in the source VRF are already imported to the receiver VRF.

SUMMARY STEPS

1. configure
2. vrf source-vrf
3. address-family [ipv4 | ipv6] unicast
4. import route-target [xx.yy:nn | as-number:nn | ip-address:nn]
5. export route-target [xx.yy:nn | as-number:nn | ip-address:nn]
6. commit
7. configure
8. vrf receiver-vrf
9. Repeat Step 3 through Step 6.
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
<td>Configures a VRF instance for the source PE router.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>vrf source-vrf</td>
<td>Configures a VRF instance for the source PE router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| | | \[
| | RP/0/RSP0/CPU0:router(config)# vrf green
| | RP/0/RSP0/CPU0:router(config-vrf)# |
| **Step 3** | address-family [ipv4 | ipv6] unicast | Specifies a unicast IPv4 or IPv6 address family and enters address family configuration submode. |
| **Note** | Only IPv4 addressing is supported for extranet. |
| **Example:** | | |
| | | \[
| | RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast |
| **Step 4** | import route-target [xx.yy:nn | as-number:nn | ip-address:nn] | Imports the selected route target, optionally expressed as one of the following:
- 4-byte AS number of the route target in \( xx.yy:nn \) format. Range is 0-65535:0-65535
- AS number of the route target in \( nn \) format. Range is 0-65535.
- IP address of the route target in \( A.B.C.D. \) format. |
| **Example:** | | |
| | | \[
| | RP/0/RSP0/CPU0:router(config-vrf-af)# import route-target 234:222
| | RP/0/RSP0/CPU0:router(config-vrf-af)# import route-target 100:100 |
| **Step 5** | export route-target [xx.yy:nn | as-number:nn | ip-address:nn] | Exports the selected route target, optionally expressed as one of the following:
- 4-byte AS number of the route target in \( xx.yy:nn \) format. Range is 0-65535:0-65535
- AS number of the route target in \( nn \) format. Range is 0-65535.
- IP address of the route target in \( A.B.C.D. \) format. |
| **Example:** | | |
| | | \[
| | RP/0/RSP0/CPU0:router(config-vrf-af)# export route-target 100:100 |
| **Step 6** | commit | | |
| **Step 7** | configure | | |
| **Step 8** | vrf receiver-vrf | Configures a VRF instance for the receiver PE router. |
| **Example:** | | |
| | | \[
| | RP/0/RSP0/CPU0:router(config)# vrf red
| | RP/0/RSP0/CPU0:router(config-vrf)# |
| **Step 9** | Repeat Step 3 through Step 6. | |
Interconnecting PIM-SM Domains with MSDP

To set up an MSDP peering relationship with MSDP-enabled routers in another domain, you configure an MSDP peer to the local router.

If you do not want to have or cannot have a BGP peer in your domain, you could define a default MSDP peer from which to accept all Source-Active (SA) messages.

Finally, you can change the Originator ID when you configure a logical RP on multiple routers in an MSDP mesh group.

Before You Begin

You must configure MSDP default peering, if the addresses of all MSDP peers are not known in BGP or multiprotocol BGP.

**SUMMARY STEPS**

1. configure
2. interface type interface-path-id
3. ipv4 address address mask
4. exit
5. router msdp
6. default-peer ip-address [prefix-list list]
7. originator-id type interface-path-id
8. peer peer-address
9. connect-source type interface-path-id
10. mesh-group name
11. remote-as as-number
12. commit
13. show msdp [ipv4] globals
14. show msdp [ipv4] peer [peer-address]
15. show msdp [ipv4] rpf rpf-address

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>(Optional) Enters interface configuration mode to define the IPv4 address for the interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong> interface type interface-path-id</td>
<td>(Optional) Defines the IPv4 address for the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# interface loopback 0</td>
<td><strong>Note</strong> This step is required if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.0.1.3 255.255.255.0</td>
<td>This step is required only if you specify an interface type and number whose primary address becomes the source IP address for the TCP connection. See optional for information about configuring the connect-source command.</td>
</tr>
</tbody>
</table>

**Step 4**

exit

**Example:** RP/0/RSP0/CPU0:router(config-if)# end

Exits interface configuration mode.

**Step 5**

router msdp

**Example:** RP/0/RSP0/CPU0:router(config)# router msdp

Enters MSDP protocol configuration mode.

**Step 6**

default-peer ip-address [prefix-list list]

**Example:** RP/0/RSP0/CPU0:router(config-msdp)# default-peer 172.23.16.0

(Optional) Defines a default peer from which to accept all MSDP SA messages.

**Step 7**

originator-id type interface-path-id

**Example:** RP/0/RSP0/CPU0:router(config-msdp)# originator-id GigabitEthernet0/1/1/0

(Optional) Allows an MSDP speaker that originates a (Source-Active) SA message to use the IP address of the interface as the RP address in the SA message.

**Step 8**

peer peer-address

**Example:** RP/0/RSP0/CPU0:router(config-msdp)# peer 172.31.1.2

Enters MSDP peer configuration mode and configures an MSDP peer.

- Configure the router as a BGP neighbor.
- If you are also BGP peering with this MSDP peer, use the same IP address for MSDP and BGP. You are not required to run BGP or multiprotocol BGP with the MSDP peer, as long as there is a BGP or multiprotocol BGP path between the MSDP peers.

**Step 9**

connect-source type interface-path-id

**Example:** RP/0/RSP0/CPU0:router(config-msdp-peer)# connect-source loopback 0

(Optional) Configures a source address used for an MSDP connection.
Controlling Source Information on MSDP Peer Routers

Your MSDP peer router can be customized to control source information that is originated, forwarded, received, cached, and encapsulated.

When originating Source-Active (SA) messages, you can control to whom you will originate source information, based on the source that is requesting information.

When forwarding SA messages you can do the following:

- Filter all source/group pairs
- Specify an extended access list to pass only certain source/group pairs
Filter based on match criteria in a route map

When receiving SA messages you can do the following:

- Filter all incoming SA messages from an MSDP peer
- Specify an extended access list to pass certain source/group pairs
- Filter based on match criteria in a route map

In addition, you can use time to live (TTL) to control what data is encapsulated in the first SA message for every source. For example, you could limit internal traffic to a TTL of eight hops. If you want other groups to go to external locations, you send those packets with a TTL greater than eight hops.

By default, MSDP automatically sends SA messages to peers when a new member joins a group and wants to receive multicast traffic. You are no longer required to configure an SA request to a specified MSDP peer.

**SUMMARY STEPS**

1. configure
2. router msdp
3. sa-filter {in | out} {ip-address | peer-name} [list access-list-name] [rp-list access-list-name]
4. cache-sa-state [list access-list-name] [rp-list access-list-name]
5. ttl-threshold ttl-value
6. exit
7. ipv4 access-list name [sequence-number] permit source [source-wildcard]
8. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters MSDP protocol configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router msdp</td>
<td>Configures an incoming or outgoing filter list for messages received from the specified MSDP peer.</td>
</tr>
</tbody>
</table>
| **Step 3** sa-filter {in | out} {ip-address | peer-name} [list access-list-name] [rp-list access-list-name] | * If you specify both the list and rp-list keywords, all conditions must be true to pass any source, group (S, G) pairs in outgoing Source-Active (SA) messages.  
| Example: | You must configure the ipv4 access-list command in **Step 7**, on page 169. |
| **Example:** | |
| RP/0/RSP0/CPU0:router(config)# router msdp | |
| RP/0/RSP0/CPU0:router(config-msdp)# sa-filter out router.cisco.com list 100 | |
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>cache-sa-state [list access-list-name] [rp-list access-list-name]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-msdp)# cache-sa-state 100</td>
</tr>
</tbody>
</table>

- Creates and caches source/group pairs from received Source-Active (SA) messages and controls pairs through access lists.

<table>
<thead>
<tr>
<th>Step 5</th>
<th>ttl-threshold ttl-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-msdp)# ttl-threshold 8</td>
</tr>
</tbody>
</table>

- (Optional) Limits which multicast data is sent in SA messages to an MSDP peer.
  - Only multicast packets with an IP header TTL greater than or equal to the `ttl-value` argument are sent to the MSDP peer specified by the IP address or name.
  - Use this command if you want to use TTL to examine your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, send those packets with a TTL greater than 8.
  - This example configures a TTL threshold of eight hops.

<table>
<thead>
<tr>
<th>Step 6</th>
<th>exit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-msdp)# exit</td>
</tr>
</tbody>
</table>

- Exits the current configuration mode.

<table>
<thead>
<tr>
<th>Step 7</th>
<th>ipv4 access-list name [sequence-number] permit source [source-wildcard]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# ipv4 access-list 100 20 permit 239.1.1.1 0.0.0.0</td>
</tr>
</tbody>
</table>

- Defines an IPv4 access list to be used by SA filtering.
  - In this example, the access list 100 permits multicast group 239.1.1.1.
  - The `ipv4 access-list` command is required if the keyword `list` is configured for SA filtering in **Step 3, on page 168**.

| Step 8 | commit |

- If all match criteria are true, a `permit` from the route map passes routes through the filter. A `deny` filters routes.
- This example allows only (S, G) pairs that pass access list 100 to be forwarded in an SA message to the peer named router.cisco.com.
Configuring MSDP MD5 Password Authentication

SUMMARY STEPS

1. configure
2. router msdp
3. peer peer-address
4. password {clear | encrypted} password
5. commit
6. show mfib [vrf vrf-name] [ipv4 | ipv6] hardware route {* | source-address | group-address[/prefix-length]} location node-id

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters MSDP configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router msdp</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config)# router msdp</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> peer peer-address</td>
<td>Configures the MSDP peer.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-msdp)# peer 10.0.5.4</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> password {clear</td>
<td>encrypted} password</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-msdp-peer)# password encrypted a34bi5m</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> commit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show mfib [vrf vrf-name] [ipv4</td>
<td>ipv6] hardware route {*</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router# show mfib hardware route * location 0/1/cpu0</td>
<td></td>
</tr>
</tbody>
</table>
Configuring VRF for MSDP

Use the `vrf` keyword in the MSDP configuration mode to enable VRF for MSDP.

**SUMMARY STEPS**

1. `configure`
2. `router msdp`
3. `vrf vrf-name`
4. `peer peer-address`
5. `commit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure</code></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>router msdp</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config)# router msdp</code></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>vrf vrf-name</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config-msdp) # vrf vrf1</code></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>peer peer-address</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>RP/0/RSP0/CPU0:router(config-msdp) # peer 1.1.1.1</code></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>commit</code></td>
</tr>
</tbody>
</table>

**Multicast only fast reroute (MoFRR)**

MoFRR allows fast reroute for multicast traffic on a multicast router. MoFRR minimizes packet loss in a network when node or link failures occur (at the topology merge point). It works by making simple enhancements to multicast routing protocols.

MoFRR involves transmitting a multicast join message from a receiver towards a source on a primary path and transmitting a secondary multicast join message from the receiver towards the source on a backup path. Data packets are received from the primary and secondary paths. The redundant packets are discarded at topology merge points with the help of Reverse Path Forwarding (RPF) checks. When a failure is detected on the primary path, the repair occurs locally by changing the interface on which packets are accepted to the...
secondary interface, thus improving the convergence times in the event of a node or link failure on the primary path.

MoFRR supports ECMP (Equal Cost Multipath) and non-ECMP topologies as well.

TI (Topology Independent) MoFRR is a multicast feature that performs fast convergence (Fast ReRoute) for specified routes/flows when failure is detected on one of the paths between the router and the source.

### Operating Modes of MoFRR

- Flow-based MoFRR—exposes the primary and secondary RPF interfaces to the forwarding plane, with switchover occurring entirely at the hardware level.

Faster convergence is obtainable in Flow-based MoFRR by monitoring the packet counts of the primary stream. If no activity is detected for 30 ms, the switch over is triggered to the backup stream and the traffic loss is within 50 ms.

### Restrictions

These limitations apply to MoFRR deployments when the Cisco ASR 9000 Series SPA Interface Processor-700 linecard is used in the Cisco ASR 9000 Series Router chassis.

1. Cisco ASR 9000 Series SPA Interface Processor-700 cannot be used on ingress interface as either the primary or backup (ECMP paths) path back to the multicast source.

2. The egress interfaces on Cisco ASR 9000 Series SPA Interface Processor-700 may lead to duplicate multicast streams for short periods of time (the time between the switch from Trident primary to Trident backup paths on ingress).

### Configuring MoFRR

#### RIB-based MoFRR

**SUMMARY STEPS**

1. configure
2. router pim
3. mofrr rib acl-name
4. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 2</th>
<th>router pim</th>
</tr>
</thead>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(config)# router pim
```

<table>
<thead>
<tr>
<th>Step 3</th>
<th>mofrr rib acl-name</th>
</tr>
</thead>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router(pim)# mofrr rib acl1
```

<table>
<thead>
<tr>
<th>Step 4</th>
<th>commit</th>
</tr>
</thead>
</table>

### Flow-based MoFRR

#### SUMMARY STEPS

1. configure
2. ipv4 access-list acl-name
3. sequence number [permit|deny] ipv4 host address [host address | any]
4. exit
5. router pim
6. mofrr acl-name
7. commit
8. show mfib hardware route summary location

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>configure</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>ipv4 access-list acl-name</th>
</tr>
</thead>
</table>

**Example:**

```
RP/0/RSP0/CPU0:router (config)# ipv4 access-list flow_mofrr
```

Enters the ACL name.

Enters the PIM configuration mode.

Enters IPv4 access list configuration mode and configures the named access list.
### Configuring MoFRR

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td>Specifies one or more conditions allowed or denied in the created IPv4 access list.</td>
</tr>
<tr>
<td>sequence number [permit</td>
<td>deny] ipv4 host address [host address</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl) #10 permit ipv4 host 20.0.0.2 any</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Saves the MoFRR acl configuration and exists the IPv4 acl configuration mode. You need to exit twice here.</td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-ipv4-acl)# exit</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enters the PIM configuration mode.</td>
</tr>
<tr>
<td>router pim</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# router pim</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Enables MoFRR for the specified access list source group with hardware switchover triggers. This is supported on IPv4 only.</td>
</tr>
<tr>
<td>mofrr acl-name</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(pim)# mofrr flow_mofrr</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>commit</td>
<td>Displays the number of enabled MoFRR routes.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>show mfib hardware route summary location</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router# show mfib hardware route 4</td>
</tr>
</tbody>
</table>
# Configuring Route Policy for Static RPF

## SUMMARY STEPS

1. `configure`
2. `router static`
3. `address-family[ipv4 | ipv6][ multicast | unicast]destination prefix interface-typeinterface-path-id`
4. `exit`
5. `route-policy policy-name`
6. `set rpf-topology policy-name address-family[ipv4 | ipv6]multicast | unicasttopologyname`
7. `end route-policy`
8. `router pim address-family[ipv4 | ipv6]`
9. `rpf topology route-policy policy-name pim policy`

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enables a static routing process.</td>
</tr>
<tr>
<td><strong>Step 2</strong> router static</td>
<td>Configures the ipv4 multicast address-family topology with a destination prefix.</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config) # router static</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> address-family[ipv4</td>
<td>ipv6][ multicast</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-static) # address-family ipv4 multicast 202.93.100.4 32 202.95.1.1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-ipv4-afi) # exit</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> route-policy policy-name</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config) # route-policy r1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> set rpf-topology policy-name address-family[ipv4</td>
<td>ipv6]multicast</td>
</tr>
<tr>
<td><strong>Example:</strong> RP/0/RSP0/CPU0:router(config-rpl) # set rpf-topology p1 ipv4 multicast topology t1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>end route-policy</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config-rpl) # end route-policy r1</code></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>`router pim address-family [ipv4</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config) # router pim address-family ipv4</code></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><code>rpf topology route-policy policy-name pim policy</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>RP/0/RSP0/CPU0:router(config) # rpf topology route-policy r1 pim policy</code></td>
</tr>
</tbody>
</table>

### Point-to-Multipoint Traffic Engineering Label-Switched Multicast

IP multicast was traditionally used for IPTV broadcasting and content delivery services. MPLS-TE (traffic engineering) is fast replacing the IP multicast technique because of the various advantages of MPLS-TE, such as:

- Fast re-routing and restoration in case of link/node failure
- Bandwidth guarantee
- Explicit path setting along with off-line computation

MPLS supports point-to-point path. However, in order to use MPLS for multicast service, MPLS has to be extended to handle point-to-multipoint paths. A reliable solution to signal Point-to-Multipoint (P2MP) label switched paths (LSP) is the Point-to-Multipoint TE LSP. This solution uses the Resource Reservation Protocol-Traffic Engineering (RSVP-TE) extension as the signaling protocol for establishing P2MP TE LSPs.

### Point to Multipoint LSP(P2MP)

P2MP LSP is unidirectional. In case of native IP multicast, the multicast forwarding always has to perform an acceptance check. This check ensures all multicast packets undergo a RPF check to ensure that the packets have arrived on the correct interface in the direction of the source. However, the acceptance check with MPLS forwarding may be different in case of an unicast or upstream label.

Depending on the multicast signaling protocol, the labeled packet may require an additional L3 lookup at the P and PE routers in order to forward the multicast packet to the physical interfaces according to multicast routing. In this case, the incoming P2MP LSP as the incoming interface for the received multicast packet must
Multicast Routing Protocol support for P2MP

All multicast routing protocols support P2MP TE LSP. At ingress node, a multicast protocol must make a mapping between the multicast traffic and the P2MP TE LSP with the configuration of static-join. At egress node, the multicast protocol must conduct a special RPF check for the multicast packet which is received from MPLS core and forward it to the customer facing interface. The RPF check is based on the configuration of static-rpf. These multicast groups which are forwarded over the P2MP TE LSPs can be specified with the static-rpf configuration in case of PIM-SSM.

Enabling Multicast Forwarding Over Tunnel Interface (at Ingress Node)

This configuration is used for allowing the forwarding of the multicast packet over the specified interface.

SUMMARY STEPS

1. configure
2. multicast-routing
3. address-family {ipv4|ipv6}
4. interface tunnel-mtc range
5. enable | disable
6. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>multicast-routing</td>
<td>Enters multicast-routing configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>interface tunnel-mte range</td>
<td>Specify the range. The range is 0 to 65535.</td>
</tr>
<tr>
<td>Example:</td>
<td>RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)#</td>
<td></td>
</tr>
</tbody>
</table>
### P2MP configurations at egress node and bud node

#### Configuring Static Reverse Path Forwarding (RPF)

**SUMMARY STEPS**

1. configure
2. multicast-routing
3. address-family {ipv4 | ipv6}
4. static-rpf address range prefix
5. mpls address
6. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>multicast-routing</td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# multicast-routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4</td>
<td></td>
</tr>
</tbody>
</table>
### Configuring Core Tree Protocol

**SUMMARY STEPS**

1. configure
2. multicast-routing
3. address-family {ipv4 | ipv6}
4. core-tree-protocol rsvp-te group-list name
5. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure</td>
<td>Enters multicast routing configuration mode.</td>
</tr>
<tr>
<td>Step 2 multicast-routing</td>
<td>Enter the source PE address of the MPLS P2MP tunnel.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 3 address-family {ipv4</td>
<td>ipv6}</td>
</tr>
<tr>
<td>Example:</td>
<td>Enter ipv4 (or ipv6)address-family submode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4 static-rpf address range prefix</td>
<td>Enter the source and prefix length.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 5 mpls address</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Step 6 commit</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 4</td>
<td>core-tree-protocol rsvp-te group-list <em>name</em></td>
</tr>
</tbody>
</table>

*Example:*

```
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)#
core-tree-protocol rsvp-te group-list acl1
```

### Step 5

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>

### Configuring IGMP VRF Override

This process consists of the following tasks:

#### Specifying VRF definition

**SUMMARY STEPS**

1. configure
2. vrf *vrf-name*
3. address-family ipv4 unicast
4. import route-target 1:1
5. export route-target 1:1
6. commit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf <em>vrf-name</em></td>
<td>Enters the VRF configuration sub mode.</td>
</tr>
</tbody>
</table>

*Example:*

```
RP/0/RSP0/CPU0:router(config)# vrf name1
```

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>address-family ipv4 unicast</td>
</tr>
</tbody>
</table>

*Example:*

```
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast
```

AFI configuration for IPv4. This is supported on unicast topologies only.
### Enabling Multicast Routing on default and non-default VRFs

This task enables multicast routing and forwarding on all new and existing interfaces. For the VRF override feature, multicast routing needs to be enabled on both, the default and the non-default VRFs.

**SUMMARY STEPS**

1. configure
2. multicast-routing vrf [vrf-name | default]
3. interface {type interface-path-id | all} enable
4. commit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure</td>
<td>Enters multicast configuration mode for the specified VRF. Note that the default configuration mode for multicast routing is default vrf (if the non-default VRF name is not specified).</td>
</tr>
<tr>
<td><strong>Step 2</strong> multicast-routing vrf [vrf-name</td>
<td>default]</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config)# multicast-routing vrf green</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface {type interface-path-id</td>
<td>all} enable</td>
</tr>
<tr>
<td>Example: RP/0/RSP0/CPU0:router(config-mcast-green)#</td>
<td></td>
</tr>
</tbody>
</table>

---

Example:

```
RP/0/RSP0/CPU0:router(config-vrf-af)# import route-target 1:1
RP/0/RSP0/CPU0:router(config-vrf-af)# export route-target 1:1
```
Configuring an Interface for a Non-default VRF Instance

SUMMARY STEPS

1. configure
2. interface type interface-path-id
3. vrf vrf-name
4. ipv4 address address mask
5. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure</td>
<td>Enters PIM address-family IPv4 submode.</td>
</tr>
<tr>
<td>interface type interface-path-id</td>
<td>Sets the VRF for the interface.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>Sets the IPv4 address for the interface.</td>
</tr>
<tr>
<td>ipv4 address address mask</td>
<td></td>
</tr>
<tr>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>
# Configuring route-policy

## SUMMARY STEPS

1. configure
2. route-policy policy-name
3. set rpf-topology vrf default
4. end-policy
5. commit

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>route-policy policy-name</td>
<td>Defines a route policy.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config)# route-policy policy1</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>set rpf-topology vrf default</td>
<td>Sets the PIM RPF topology attributes for the default VRF.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-rpl)# set rpf-topology vrf default</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>end-policy</td>
<td>Ends the route-policy definition configuration.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-rpl)# end-policy</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>commit</td>
<td></td>
</tr>
</tbody>
</table>
Associating a route policy to PIM configuration for the VRF receiving IGMP reports

SUMMARY STEPS

1. configure
2. `router pim vrf vrf-name address-family ipv4`
3. `rpf-topology route-policy policy-name`
4. commit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>router pim vrf vrf-name address-family ipv4</code></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>rpf-topology route-policy policy-name</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td>RP/0/RSP0/CPU0:router(config-rpl)# rpf-topology extranet-igmp-reports</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>commit</td>
</tr>
</tbody>
</table>

Configuration Examples for Implementing Multicast Routing on Software

This section provides the following configuration examples:

Calculating Rates per Route: Example

The following example illustrates output from hardware counters based on rate per route for a specific source and group address location:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# multicast-routing vrf vpn12 address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# rate-per-route
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface all enable
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# accounting per-prefix
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# commit
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# exit
```
Preventing Auto-RP Messages from Being Forwarded on Software: Example

This example shows that Auto-RP messages are prevented from being sent out of the GigabitEthernet interface 0/3/0/0. It also shows that access list 111 is used by the Auto-RP candidate and access list 222 is used by the boundary command to contain traffic on GigabitEthernet interface 0/3/0/0.

```
ipv4 access-list 111
10 permit 224.1.0.0 0.0.255.255 any
20 permit 224.2.0.0 0.0.255.255 any
!
!Access list 111 is used by the Auto-RP candidate.
!
ipv4 access-list 222
10 deny any host 224.0.1.39
20 deny any host 224.0.1.40
!
!Access list 222 is used by the boundary command to contain traffic (on
```
GigabitEthernet0/3/0/0) that is sent to groups 224.0.1.39 and 224.0.1.40.

router pim
  auto-rp mapping-agent loopback 2 scope 32 interval 30
  auto-rp candidate-rp loopback 2 scope 15 group-list 111 interval 30
  multicast-routing
    interface GigabitEthernet0/3/0/0
    boundary 222

Inheritance in MSDP on Software: Example

The following MSDP commands can be inherited by all MSDP peers when configured under router MSDP configuration mode. In addition, commands can be configured under the peer configuration mode for specific peers to override the inheritance feature.

- connect-source
- sa-filter
- ttl-threshold

If a command is configured in both the router msdp and peer configuration modes, the peer configuration takes precedence.

In the following example, MSDP on Router A filters Source-Active (SA) announcements on all peer groups in the address range 226/8 (except IP address 172.16.0.2); and filters SAs sourced by the originator RP 172.16.0.3 to 172.16.0.2.

MSDP peers (172.16.0.1, 172.16.0.2, and 172.17.0.1) use the loopback 0 address of Router A to set up peering. However, peer 192.168.12.2 uses the IPv4 address configured on the GigabitEthernet interface to peer with Router A.

Router A

ipv4 access-list 111
  10 deny ip host 172.16.0.3 any
  20 permit any any

ipv4 access-list 112
  10 deny any 226.0.0.0 0.255.255.255
  30 permit any any

router msdp
  connect-source loopback 0
  sa-filter in rp-list 111
  sa-filter out rp-list 111
  peer 172.16.0.1
    peer 172.16.0.2
    sa-filter out list 112
    peer 172.17.0.1
    peer 192.168.12.2
      connect-source GigabitEthernet0/2/0/0
MSDP-VRF: Example

This is an example where, peer 1.1.1.1 is configured in the VRF context for vrf1.

```
config
router msdp
  vrf vrf1
    peer 1.1.1.1
exit
end
```

Configuring Route Policy for Static RPF: Example

```
router static
  address-family ipv4 multicast
    202.93.192.74 /32 202.40.148.11

! route-policy pim-policy
  set rpf-topology ipv4 multicast topology default
end-policy
!
router pim
  address-family ipv4
    rpf topology route-policy pim-policy
```

Configuring IPv4 Multicast VPN: Example

Cisco ASR 9000 Series Routers support only IPv4 addressing.

This end-to-end configuration example shows how to establish a multicast VPN topology (Figure 12: Topology in CE4PE1PE2 CE3MVPN Configuration, on page 187), using two different routing protocols (OSPF or BGP) to broadcasting traffic between customer-edge(CE) routers and provider-edge (PE) routers:

```
Figure 12: Topology in CE4PE1PE2 CE3MVPN Configuration

CE4------------------ PE1 ------------------------------------------------ PE2 ------------------ CE3

For more configuration information, see the Configuring Multicast VPN, on page 116 of this module and also related configuration information in Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide.

Configuring MVPN to Advertise Routes Between the CE and the PE Using OSPF: Example

PE1:

```
! vrf vpn1
  address-family ipv4 unicast
  import route-target
```
1:1
!
export route-target
1:1
!
!
interface Loopback0
ipv4 address 1.1.1.1 255.255.255.255
!
interface Loopback1
vrf vpn1
ipv4 address 2.2.2.2 255.255.255.255
!
interface GigabitEthernet0/5/0/0
vrf vpn1
ipv4 address 101.1.1.1 255.255.255.0
!
interface TenGigE0/6/0/0
ipv4 address 12.1.1.1 255.255.255.0
!
mpls ldp
router-id 1.1.1.1
!
!
multicast-routing
vrf vpn1 address-family ipv4
mdt data 233.1.0.0/16 threshold 3
mdt default ipv4 232.1.1.1
rate-per-route
interface all enable
accounting per-prefix
!
address-family ipv4
nsf
mdt source Loopback0
interface all enable
accounting per-prefix
!
!
router bgp 100
bgp router-id 1.1.1.1
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
address-family ipv4 mdt
!
neighbor 9.9.9.9
remote-as 100
update-source Loopback0
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
address-family ipv4 mdt
!
!
! vrf vpn1
rd 1:1
address-family ipv4 unicast
redistribute ospf 1
!
!
router ospf 1
vrf vpn1
router-id 2.2.2.2
redistribute bgp 100
area 0
interface Loopback1
!
interface GigabitEthernet0/5/0/0
  !
  !
router ospf 100
  router-id 1.1.1.1
  area 0
    interface Loopback0
    !
    interface TenGigE0/6/0/0
    !
  !
router pim vrf vpn1 address-family ipv4
  rp-address 2.2.2.2
  log neighbor changes
  !
router pim vrf default address-family ipv4
  rp-address 1.1.1.1
  !
end

PE2:

! vrf vpn1
  address-family ipv4 unicast
    import route-target
    1:1
    !
    export route-target
    1:1
    !
  !
  interface Loopback0
    ipv4 address 9.9.9.9 255.255.255.255
  !
  interface Loopback1
    vrf vpn1
    ipv4 address 10.10.10.10 255.255.255.255
  
  interface GigabitEthernet0/2/2/7
    vrf vpn1
    ipv4 address 122.1.1.1 255.255.255.0
    negotiation auto
  
  interface TenGigE0/3/0/0
    ipv4 address 12.1.1.2 255.255.255.0
  
  mpls ldp
  router-id 9.9.9.9
  interface TenGigE0/3/0/0
  
  !
  multicast-routing
  vrf vpn1 address-family ipv4
    mdt data 233.1.0.0/16 threshold 3
    mdt default ipv4 232.1.1.1
    rate-per-route
    interface all enable
    accounting per-prefix
    !
  address-family ipv4
  nsf
  mdt source Loopback0
  interface all enable
  accounting per-prefix
  !
router bgp 100
  bgp router-id 9.9.9.9
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
  address-family ipv4 mdt
  !
  neighbor 1.1.1.1
    remote-as 100
    update-source Loopback0
  address-family ipv4 unicast
    !
  address-family vpnv4 unicast
    !
  address-family ipv4 mdt
  !
  vrf vpn1
    rd 1:1
    address-family ipv4 unicast
    redistribute ospf 1
    !
  !
  router ospf 1
  vrf vpn1
    router-id 10.10.10.10
    redistribute bgp 100
    area 0
    interface Loopback1
    !
    interface GigabitEthernet0/2/2/7
    !
  !
  router ospf 100
  router-id 9.9.9.9
  area 0
  interface Loopback0
  !
  interface TenGigE0/3/0/0
  !
  !
  router pim vrf vpn1 address-family ipv4
    rp-address 2.2.2.2
  !
  router pim vrf default address-family ipv4
    rp-address 1.1.1.1
  !
  end

CE4:

For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software configuration documentation.

interface Loopback0
  ipv4 address 101.101.101.101 255.255.255.255
interface GigabitEthernet0/0/0/0
  ipv4 address 101.1.1.2 255.255.255.0
interface GigabitEthernet0/0/0/3
  ipv4 address 11.1.1.1 255.255.255.0
multicast-routing
address-family ipv4
  interface all enable

! router ospf 1
  router-id 101.101.101.101
  area 0
    interface Loopback0
    ! interface GigabitEthernet0/0/0/0
    ! interface GigabitEthernet0/0/0/3
    !
    !
  router pim vrf default address-family ipv4
    rp-address 2.2.2.2
    interface Loopback0
    ! interface GigabitEthernet0/0/0/0
    ! interface GigabitEthernet0/0/0/3
    !
    !
end

CE3:

For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software configuration documentation.

interface Loopback0
  ipv4 address 122.122.122.122 255.255.255.255
  !
interface GigabitEthernet0/1/3/0
  ipv4 address 22.1.1.1 255.255.255.0
  !
interface GigabitEthernet0/2/3/0
  ipv4 address 122.1.1.2 255.255.255.0
  multicast-routing
  address-family ipv4
  interface all enable
  ! router ospf 1
  router-id 122.122.122.122
  area 0
    interface Loopback0
    ! interface GigabitEthernet0/1/3/0
    ! interface GigabitEthernet0/2/3/0
    !
    !
  router pim vrf default address-family ipv4
    rp-address 2.2.2.2
    interface Loopback0
    ! interface GigabitEthernet0/1/3/0
    ! interface GigabitEthernet0/2/3/0
    !
    !
end
Configuring MVPN to Advertise Routes Between the CE and the PE Using BGP: Example

PE1:

vrf vpn1
    address-family ipv4 unicast
        import route-target
        1:1
        export route-target
        1:1

interface Loopback0
    ipv4 address 1.1.1.1 255.255.255.255

interface Loopback1
    vrf vpn1
    ipv4 address 2.2.2.2 255.255.255.255

interface GigabitEthernet0/5/0/0
    vrf vpn1
    ipv4 address 101.1.1.1 255.255.255.0

interface TenGigE0/6/0/0
    ipv4 address 12.1.1.1 255.255.255.0

mpls ldp
    router-id 1.1.1.1

interface TenGigE0/6/0/0
    enable

multicast-routing
    vrf vpn1 address-family ipv4
        mdt data 233.1.0.0/16 threshold 3
        mdt default ipv4 232.1.1.1
        rate-per-route
        interface all enable
        accounting per-prefix
        !
        address-family ipv4
        !
        mdt source Loopback0
        interface all enable
        accounting per-prefix
        !
        route-policy pass-all
            pass
        end-policy
    !
    router bgp 100
    bgp router-id 1.1.1.1
        address-family ipv4 unicast
        !
        address-family vpnv4 unicast
        !
        address-family ipv4 mdt
        !
        neighbor 9.9.9.9
            remote-as 100
            update-source Loopback0
            address-family ipv4 unicast
            !
            address-family vpnv4 unicast
            !
            address-family ipv4 mdt
            !
PE2:

vrf vpn1
address-family ipv4 unicast
import route-target 1:1
export route-target 1:1

interface Loopback0
ipv4 address 9.9.9.9 255.255.255.255

interface Loopback1
vrf vpn1
ipv4 address 10.10.10.10 255.255.255.255

interface GigabitEthernet0/2/2/7
vrf vpn1
ipv4 address 122.1.1.1 255.255.255.0
negotation auto

interface TenGigE0/3/0/0
ipv4 address 12.1.1.2 255.255.255.0

mpls ldp
router-id 9.9.9.9

interface TenGigE0/3/0/0
multicast-routing
vrf vpn1 address-family ipv4
mdt data 233.1.0.0/16 threshold 3
mdt default ipv4 232.1.1.1
rate-per-route
interface all enable
accounting per-prefix
!
address-family ipv4
nsf
mdt source Loopback0
interface all enable
accounting per-prefix
!
!
route-policy pass-all
pass
end-policy
!
router bgp 100
bgp router-id 9.9.9.9
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
address-family ipv4 mdt
!
neighbor 1.1.1.1
remote-as 100
update-source Loopback0
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
address-family ipv4 mdt
!
!
vrf vpn1
rd 1:1
address-family ipv4 unicast
redistribute connected
!
neighbor 122.1.1.2
remote-as 500
address-family ipv4 unicast
route-policy pass-all in
route-policy pass-all out
!
!
router ospf 100
router-id 9.9.9.9
area 0
interface Loopback0
!
interface TenGigE0/3/0/0
!
!
router pim vrf vpn1 address-family ipv4
rp-address 2.2.2.2
!
router pim vrf default address-family ipv4
rp-address 1.1.1.1
!
end
CE4:
For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software configuration documentation.

```plaintext
interface Loopback0
  ipv4 address 101.101.101.101 255.255.255.255
!
interface GigabitEthernet0/0/0/0
  ipv4 address 101.1.1.2 255.255.255.0
!
interface GigabitEthernet0/0/0/3
  ipv4 address 11.1.1.1 255.255.255.0
!
multicast-routing
  address-family ipv4
    interface all enable
  
!
route-policy pass-all
  pass
end-policy
!
router bgp 400
  bgp router-id 101.101.101.101
  address-family ipv4 unicast
    redistribute connected
  
neighbor 101.1.1.1
  remote-as 100
  address-family ipv4 unicast
  route-policy pass-all in
  route-policy pass-all out
  
!
router pim vrf default address-family ipv4
  rp-address 2.2.2.2
interface Loopback0
  
interface GigabitEthernet0/0/0/0
  
interface GigabitEthernet0/0/0/3
  
end
```

CE3:
For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software configuration documentation.

```plaintext
interface Loopback0
  ipv4 address 122.122.122.122 255.255.255.255
!

interface GigabitEthernet0/1/3/0
  ipv4 address 22.1.1.1 255.255.255.0
!

interface GigabitEthernet0/2/3/0
  ipv4 address 122.1.1.2 255.255.255.0

multicast-routing
  address-family ipv4
    interface all enable
```

---

**Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide, Release 4.2.x**

195
Configuration Examples for MVPN Profiles

The profile-wise configuration examples for the various MVPN profiles.

Configuration Examples for Inband mLDP profiles

Profile-6: VRF Inband mLDP

router bgp 100
  mvpn
  !
  multicast-routing
  mdt source Loopback0
  vrf v61
    address-family ipv4
      mdt mtu 1600
      mdt mldp in-band-signaling ipv4
      interface all enable
    !
    address-family ipv6
      mdt mtu 1600
      mdt mldp in-band-signaling ipv4
      interface all enable
    !
  router pim
    vrf v61
      address-family ipv4
        rpf topology route-policy mldp-inband
      !
      address-family ipv6
        rpf topology route-policy mldp-inband
      !
    route-policy mldp-inband
    set core-tree mldp-inband
Profile-7: Global Inband mLDP

```conf
end-policy
!
```

```conf
multicast-routing
  address-family ipv4
    mdt source Loopback0
    mdt mldp in-band-signaling ipv4
    ssm range Global-SSM-Group
    interface all enable
  !
  address-family ipv6
    mdt source Loopback0
    mdt mldp in-band-signaling ipv4
    ssm range Global-SSM-Group-V6
    interface all enable
  !
  router pim
    address-family ipv4
      rpf topology route-policy mldp-inband
    !
    address-family ipv6
      rpf topology route-policy mldp-inband
      
      route-policy mldp-inband
      set core-tree mldp-inband
end-policy
```

### Configuration Examples for P2MP-TE profiles

**Profile-8: Global Static P2MP-TE**

```conf
interface Loopback0
  ipv4 address 200.200.1.1 255.255.255.255
!
multicast-routing
  address-family ipv4
    mdt source Loopback0
    ssm range Global-SSM-Group
    interface all enable
  !
  address-family ipv6
    mdt source Loopback0
    ssm range Global-SSM-Group-V6
    interface all enable
  !
  router igmp
    interface tunnel-mte1
      static-group 228.1.1.1 2.2.2.1
    !
  router mld
    interface tunnel-mte1
    static-group ff3e:0:228::1 2001:2:2:2::1
```

**Profile-10: VRF static P2MP-TE with BGP-AD**

```conf
! multicast-routing
  mdt source Loopback0
  vrf v101
    address-family ipv4
      mdt static p2mp-te tunnel-mte10
      interface all enable
    bgp auto-discovery p2mp-te
    !
  router igmp
  vrf v101
  interface tunnel-mte10
```
static-group 227.101.1.1 101.7.1.1
!

Profile-18: Rosen Static P2MP-TE with BGP-AD and PIM signaling

multicast-routing
 mdt source Loopback0
 vrf v181
  address-family ipv4
   mdt default p2mp-te static tunnel-mte18
   interface all enable
   bgp auto-discovery p2mp-te
 !
  address-family ipv6
   mdt default p2mp-te static tunnel-mte181
   interface all enable
   bgp auto-discovery p2mp-te
 !
 router pim
  vrf v181
   address-family ipv4
    rpf topology route-policy p2mp-te-default
 !
   address-family ipv6
    rpf topology route-policy p2mp-te-default
 !
  route-policy p2mp-te-default
   set core-tree p2mp-te-default
 end-policy
!

Profile-16: Rosen Static P2MP-TE with BGP-Ad and BGP signaling
!
multicast-routing
 mdt source Loopback0
 vrf v161
  address-family ipv4
   mdt default p2mp-te static tunnel-mte16
   interface all enable
   bgp auto-discovery p2mp-te
 !
  address-family ipv6
   mdt default p2mp-te static tunnel-mte161
   interface all enable
   bgp auto-discovery p2mp-te
 !
 router pim
  vrf v161
   address-family ipv4
    rpf topology route-policy p2mp-te-default
    mdt c-multicast-routing bgp
 !
   address-family ipv6
    rpf topology route-policy p2mp-te-default
    mdt c-multicast-routing bgp
 !
  route-policy p2mp-te-default
   set core-tree p2mp-te-default
 end-policy
!
Configuration examples for Partitioned mLDP profiles

Profile-2: Partitioned mLDP MP2MP without BGP-AD

```
router bgp 100
  mvpn
  !
  multicast-routing
  vrf v21
    address-family ipv4
      mdt mtu 1600
      mdt partitioned mldp ipv4 mp2mp
      interface all enable
    !
    address-family ipv6
      mdt mtu 1600
      mdt partitioned mldp ipv4 mp2mp
      interface all enable
    !
  !
  router pim
  vrf v21
    address-family ipv4
      rpf topology route-policy mldp-partitioned-mp2mp
    !
    address-family ipv6
      rpf topology route-policy mldp-partitioned-mp2mp
    !
  !
  route-policy mldp-partitioned-mp2mp
    set core-tree mldp-partitioned-mp2mp
  end-policy
```

Profile-4: Partitioned mLDP MP2MP with BGP-AD and PIM signaling

```
! 
  multicast-routing
  mdt source Loopback0
  vrf v41
    address-family ipv4
      mdt mtu 1600
    mdt partitioned mldp ipv4 mp2mp
    mdt data 255
      interface all enable
      bgp auto-discovery mldp
    !
    address-family ipv6
      mdt mtu 1600
    mdt partitioned mldp ipv4 mp2mp
    mdt data 255
      interface all enable
      bgp auto-discovery mldp
    !
  !
  router pim
  vrf v41
    address-family ipv4
      rpf topology route-policy mldp-partitioned-mp2mp
    !
    address-family ipv6
      rpf topology route-policy mldp-partitioned-mp2mp
    !
  !
  route-policy mldp-partitioned-mp2mp
    set core-tree mldp-partitioned-mp2mp
  end-policy
```
Profile-15: Partitioned mLDP MP2MP with BGP-AD and BGP signaling

```
multicast-routing
  mdt source Loopback0
vrf v151
    address-family ipv4
      mdt mtu 1600
    mdt partitioned mldp ipv4 mp2mp
    mdt data 255
      interface all enable
      bgp auto-discovery mldp
    address-family ipv6
      mdt mtu 1600
    mdt partitioned mldp ipv4 mp2mp
    mdt data 255
      interface all enable
      bgp auto-discovery mldp
  router pim
    vrf v151
      address-family ipv4
        rpf topology route-policy mldp-partitioned-mp2mp
        mdt c-multicast-routing bgp
      address-family ipv6
        rpf topology route-policy mldp-partitioned-mp2mp
        mdt c-multicast-routing bgp
    route-policy mldp-partitioned-mp2mp
      set core-tree mldp-partitioned-mp2mp
    end-policy
```

Profile-5: Partitioned mLDP P2MP with BGP-AD and PIM signaling

```
multicast-routing
  mdt source Loopback0
vrf v51
  address-family ipv4
    mdt mtu 1600
  mdt partitioned mldp ipv4 p2mp
  mdt data 255
    interface all enable
    bgp auto-discovery mldp
  address-family ipv6
    mdt mtu 1600
  mdt partitioned mldp ipv4 p2mp
  mdt data 255
    interface all enable
    bgp auto-discovery mldp
  router pim
    vrf v51
      address-family ipv4
        rpf topology route-policy mldp-partitioned-p2mp
      address-family ipv6
        rpf topology route-policy mldp-partitioned-p2mp
    route-policy mldp-partitioned-p2mp
      set core-tree mldp-partitioned-p2mp
    end-policy
```

Profile-14: Partitioned mLDP P2MP with BGP-AD and BGP signaling

```
multicast-routing
```
Configuration Examples for Rosen-mGRE profiles

Profile-0: Rosen mGRE with MDT SAFI

router bgp 100
  address-family ipv4 mdt
  neighbor X.X.X.X < -----RR or Remote PE ip address
  address-family ipv4 mdt

  multicast-routing
  address-family ipv4
    mdt source Loopback0
    interface all enable
  !
  address-family ipv6
    mdt source Loopback0
    interface all enable
  !
  vrf v1
  address-family ipv4
    mdt mtu 1600
    mdt data 231.1.1.2/32
    mdt default ipv4 231.1.1.1
    interface all enable
  !
  address-family ipv6
    mdt mtu 1600
    mdt data 231.1.1.2/32
    mdt default ipv4 231.1.1.1
    interface all enable
  !
Profile-3: Rosen mGRE with BGP-AD and PIM signaling

```
router bgp 100
  
  address-family ipv4 mvpn
  !
  address-family ipv6 mvpn
  !
  neighbor X.X.X.X < ----> RR or Remote PE ip address
    address-family ipv4 mvpn
    !
    address-family ipv6 mvpn
    !
  !
  vrf v31
    rd 100:31
    address-family ipv4 mvpn
    !
    address-family ipv6 mvpn
    !
    !
    multicast-routing
    mdt source Loopback0
    vrf v31
      address-family ipv4
      mdt mtu 1600
      mdt data 232.31.1.2/32
      mdt default ipv4 232.31.1.1
      interface all enable
      bgp auto-discovery pim
      !
      address-family ipv6
      mdt mtu 1600
      mdt data 232.31.1.2/32
      mdt default ipv4 232.31.1.1
      interface all enable
      bgp auto-discovery pim
      !
```

Profile-11: Rosen mGRE with BGP-AD and BGP signaling

```
router bgp 100
  
  address-family ipv4 mvpn
  !
  address-family ipv6 mvpn
  !
  neighbor X.X.X.X < ----> RR or Remote PE ip address
    address-family ipv4 mvpn
    !
    address-family ipv6 mvpn
    !
  !
  vrf v111
    rd 100:111
    address-family ipv4 mvpn
    !
    address-family ipv6 mvpn
    !
    !
    multicast-routing
    mdt source Loopback0
    vrf v111
      address-family ipv4
      mdt mtu 1600
      mdt data 232.111.1.2/32
      mdt default ipv4 232.111.1.1
      interface all enable
      bgp auto-discovery pim
      !
      address-family ipv6
```

Implementing Layer-3 Multicast Routing on Cisco IOS XR Software
Configuration Examples for MVPN Profiles
Cisco ASR 9000 Series Aggregation Services Router Multicast Configuration Guide, Release 4.2.x
Configuration Examples for Rosen mLDP profiles

Profile-1: Rosen mLDP with M2MP without BGP-AD

vrf v11
  vpn id 100:11
  router bgp 100
  mvpn
  !
  multicast-routing
  mdt source Loopback0
  vrf v11
  address-family ipv4
    mdt mtu 1600
    mdt default mldp ipv4 100.100.1.1
    mdt default mldp ipv4 100.100.1.2
    mdt data 255
    interface all enable
    !
  address-family ipv6
    mdt mtu 1600
    mdt default mldp ipv4 100.100.1.1
    mdt default mldp ipv4 100.100.1.2
    mdt data 255
    interface all enable
    !
  router pim
  vrf v11
  address-family ipv4
    rpf topology route-policy rosen-mldp
    !
  address-family ipv6
    rpf topology route-policy rosen-mldp
    !
  !
  route-policy rosen-mldp
  set core-tree mldp-default
  end-policy!

Profile-9: Rosen mLDP MP2MP with BGP-AD and PIM signaling

vrf v91
  vpn id 100:91
  !
  !
  multicast-routing
  mdt source Loopback0
  vrf v91
  address-family ipv4
    mdt mtu 1600
    mdt default mldp ipv4 100.100.1.1
    mdt default mldp ipv4 100.100.1.2
  !
  address-family ipv6
    mdt mtu 1600
    mdt default mldp ipv4 100.100.1.1
    mdt default mldp ipv4 100.100.1.2
Configuration Examples for MVPN Profiles

Profile-13: Rosen mLDP MP2MP with BGP-AD and BGP signaling

vrf v131
vpn id 100:131
!
multicast-routing
mtd source Loopback0
vrf v131
address-family ipv4
mtd mtu 1600
mtd default mldp ipv4 100.100.1.1
mtd default mldp ipv4 100.100.1.2
mtd data 255
interface all enable
bgp auto-discovery mldp
!
address-family ipv6
mtd mtu 1600
mtd default mldp ipv4 100.100.1.1
mtd default mldp ipv4 100.100.1.2
mtd data 255
interface all enable
bgp auto-discovery mldp
!
router pim
vrf v91
address-family ipv4
  rpf topology route-policy rosen-mldp
!
  address-family ipv6
  rpf topology route-policy rosen-mldp
!
route-policy rosen-mldp
  set core-tree mldp-default
end-policy

Profile-17: Rosen mLDP P2MP with BGP-AD and PIM signaling

vrf v171
vpn id 100:131
!
multicast-routing
mtd source Loopback0
vrf v171
address-family ipv4
mtd mtu 1600
mtd default mldp ipv4 100.100.1.1
mtd default mldp ipv4 100.100.1.2
mtd data 255
interface all enable
bgp auto-discovery mldp
!
route-policy rosen-mldp
mtd c-multicast-routing bgp
!
route-policy rosen-mldp
mtd c-multicast-routing bgp
!
route-policy rosen-mldp
  set core-tree mldp-default
end-policy
vrf v171
  address-family ipv4
    mdt mtu 1600
    mdt default mldp p2mp
    mdt data 255
    interface all enable
    bgp auto-discovery mldp
  !
  address-family ipv6
    mdt mtu 1600
    mdt default mldp p2mp
    mdt data 255
    interface all enable
    bgp auto-discovery mldp
  !
router pim
  vrf v171
  address-family ipv4
    rpf topology route-policy rosen-mldp
  !
  address-family ipv6
    rpf topology route-policy rosen-mldp
  !
route-policy rosen-mldp
  set core-tree mldp-default
end-policy

Profile-12: Rosen mLDP P2MP with BGP-AD and BGP signaling

! multicast-routing
  mdt source Loopback0
  vrf v121
    address-family ipv4
      mdt mtu 1600
      mdt default mldp p2mp
      mdt data 255
      interface all enable
      bgp auto-discovery mldp
  !
  address-family ipv6
    mdt mtu 1600
    mdt default mldp p2mp
    mdt data 255
    interface all enable
    bgp auto-discovery mldp
  !
router pim
  vrf v121
    address-family ipv4
      rpf topology route-policy rosen-mldp
    mdt c-multicast-routing bgp
  !
    address-family ipv6
      rpf topology route-policy rosen-mldp
    mdt c-multicast-routing bgp
  !
route-policy rosen-mldp
  set core-tree mldp-default
end-policy
Configuring MVPN Static P2MP TE: Examples

Configuring MVPN P2MP on Ingress PE: Example

```plaintext
configure
multicast-routing
address-family ipv4
mdt source Loopback0
interface all enable
!
set vrf vrf1
address-family ipv4
bgp auto-discovery rsvpte
mdt static p2mp-te tunnel-mte1
interface all enable
!
router igmp
vrf vrf1
interface tunnel-mte1
static-group 232.1.1.1 192.1.1.2
!
```

Configuring MVPN P2MP BGP: Example

```plaintext
router bgp 100
bgp router-id 110.110.110.110
address-family ipv4 unicast
address-family vpnv4 unicast
address-family ipv4 mvpn
!
neighbor 130.130.130.130
remote-as 100
update-source Loopback0
address-family ipv4 unicast
address-family vpnv4 unicast
address-family ipv4 mvpn
!
set vrf vrf1
rd 1:1
bgp router-id 110.110.110.110
address-family ipv4 unicast
redistribute connected
address-family ipv4 mvpn
!
```

Configuring MVPN P2MP on Egress PE: Example

```plaintext
multicast-routing
address-family ipv4
mdt source Loopback0
interface all enable
!
set vrf vrf1
address-family ipv4
core-tree-protocol rsvp-te group-list mvpn-acl
interface all enable
!
ipv4 access-list mvpn-acl
10 permit ipv4 host 192.1.1.2 host 232.1.1.1
```
20 permit ipv4 any host 232.1.1.2

Configuring MVPN Extranet Routing: Example

These examples describe two ways to configure MVPN extranet routing:
For the full set of configuration tasks, see Configuring MVPN Extranet Routing, on page 162.

Configuring the Source MVRF on the Receiver PE Router: Example

The following examples show how to configure MVPN extranet routing by specifying the source MVRF on the receiver PE router.
You must configure both the source PE router and the receiver PE router.

Configure the Source PE Router Using Route Targets

```
interface Loopback5
  ipv4 address 201.5.5.201 255.255.255.255
!
interface Loopback22
  vrf provider-vrf
  ipv4 address 201.22.22.201 255.255.255.255
!
interface GigabitEthernet0/6/0/0
  vrf provider-vrf
  ipv4 address 10.10.10.1 255.255.0.0
!
  vrf provider-vrf
  address-family ipv4 unicast
  import route-target
  1100:1
  export route-target
  1100:1
! router bgp 1
  regular BGP MVPN config
  vrf provider-vrf
  rd 1100:1
  address-family ipv4 unicast
  redistribute connected
!
!
  multicast-routing
  vrf provider-vrf address-family ipv4
  mdt data 226.1.4.0/24 threshold 3
  log-traps
  mdt default ipv4 226.0.0.4
  rate-per-route
  interface all enable
  accounting per-prefix
!
! address-family ipv4
  nsf
  mdt source Loopback5
  interface all enable
!
! router pim vrf provider-vrf address-family ipv4
  rp-address 201.22.22.201
```
Configure the Receiver PE Router Using Route Targets

interface Loopback5
  ipv4 address 202.5.5.202 255.255.255.255

interface GigabitEthernet0/3/0/2
  vrf receiver-vrf
  ipv4 address 20.20.20.1 255.255.0.0

  vrf provider-vrf
    address-family ipv4 unicast
    import route-target 1100:1
    export route-target 1100:1

  vrf receiver-vrf
    address-family ipv4 unicast
    import route-target
    export route-target

  multicast-routing
    vrf provider-vrf address-family ipv4
      log-traps
      mdt default ipv4 226.0.0.4
      rate-per-route
      interface all enable
      accounting per-prefix

    vrf receiver_vrf address-family ipv4
      log-traps
      mdt default ipv4 226.0.0.5
      rate-per-route
      interface all enable
      accounting per-prefix

    address-family ipv4
      nsf
      mdt source Loopback5
      interface all enable

  router pim vrf provider-vrf address-family ipv4
    rp-address 201.22.22.201

  router pim vrf receiver_vrf address-family ipv4
    rp-address 201.22.22.201

  router bgp 1
    regular BGP MVPN config
    vrf provider-vrf
      rd 1100:1
      address-family ipv4 unicast
      redistribute connected

    vrf receiver_vrf
      rd 1101:1
      address-family ipv4 unicast
      redistribute connected
Configuring RPL Policies in Receiver VRFs to Propagate Joins to a Source VRF: Example

In addition to configuring route targets, Routing Policy Language (RPL) policies can be configured in receiver VRFs on receiver PE routers to propagate joins to a specified source VRF. However, this configuration is optional.

The following configuration example shows a policy where the receiver VRF can pick either “provider_vrf_1” or “provider_vrf_2” to propagate PIM joins.

In this example, provider_vrf_1 is used for multicast streams in the range of from 227.0.0.0 to 227.255.255.255, while provider_vrf_2 is being used for streams in the range of from 228.0.0.0 to 228.255.255.255.

```plaintext
route-policy extranet_streams_from_provider_vrf
  if destination in (227.0.0.0/32 ge 8 le 32) then
    set rpf-topology vrf provider_vrf_1
  elseif destination in (228.0.0.0/32 ge 8 le 32) then
    set rpf-topology vrf provider_vrf_2
  else
    pass
  endif
end-policy

router pim vrf receiver_vrf address-family ipv4
  rpf topology route-policy extranet_streams_from_provider_vrf
```

Configuring the Receiver MVRF on the Source PE Router: Example

The following examples show how to configure MVPN extranet routing by specifying the receiver MVRF on the source PE router.

---

**Note**
You must configure both the source PE router and the receiver PE router.

---

Configure the Source PE Router Using Route Targets

```plaintext
interface Loopback5
  ipv4 address 202.5.5.202 255.255.255.255

interface GigabitEthernet0/3/0/2
  vrf provider-vrf
  ipv4 address 20.20.20.1 255.255.0.0

vrf provider-vrf
  address-family ipv4 unicast
  import route-target 1100:1

vrf receiver-vrf
  address-family ipv4 unicast
  import route-target 1100:1
```
1101:1
!
export route-target
1101:1
!

router bgp 1
regular BGP MVPN config
vrf provider-vrf
rd 1100:1
address-family ipv4 unicast
redistribute connected
!
vrf receiver-vrf
rd 1101:1
address-family ipv4 unicast
redistribute connected
!

multicast-routing
vrf provider-vrf address-family ipv4
log-traps
mdt default ipv4 226.0.0.4
rate-per-route
interface all enable
accounting per-prefix
!
vrf receiver_vrf address-family ipv4
log-traps
mdt default ipv4 226.0.0.5
rate-per-route
interface all enable
accounting per-prefix
!
address-family ipv4
nsf
mdt source Loopback5
interface all enable
!
router pim vrf provider-vrf address-family ipv4
rp-address 201.22.22.201
!
router pim vrf receiver_vrf address-family ipv4
rp-address 201.22.22.201
!

Configure the Receiver PE Router Using Route Targets

interface Loopback5
ipv4 address 201.5.5.201 255.255.255.255
!
interface Loopback22
vrf receiver_vrf
ipv4 address 201.22.22.201 255.255.255.255
!
interface GigabitEthernet0/6/0
vrf receiver_vrf
ipv4 address 10.10.10.1 255.255.0.0
!

vrf receiver_vrf
address-family ipv4 unicast
import route-target
1100:1
1101:1
!
export route-target 1101:1
!

router bgp 1
  regular BGP MVPN config
  vrf receiver_vrf
  rd 1101:1
  address-family ipv4 unicast
  redistribute connected
!
multicast-routing
  vrf receiver_vrf address-family ipv4
  log-traps
  mdt default ipv4 226.0.0.5
  rate-per-route
  interface all enable
  accounting per-prefix
!
  address-family ipv4
  nsf
  mdt source Loopback5
  interface all enable
!

router pim vrf receiver_vrf address-family ipv4
  rp-address 201.22.22.201
!

### Configuring RPL Policies in Receiver VRFs on Source PE Routers to Propagate Joins to a Source VRF: Example

In addition to configuring route targets, RPL policies can be configured in receiver VRFs on a source PE router to propagate joins to a specified source VRF. However, this configuration is optional.

The configuration below shows a policy in which the receiver VRF can select either "provider_vrf_1" or "provider_vrf_2" to propagate PIM joins. Provider_vrf_1 will be selected if the rendezvous point (RP) for a multicast stream is 201.22.22.201, while provider_vrf_2 will be selected if the RP for a multicast stream is 202.22.22.201.

As an alternative, you can configure a multicast group-based policy as shown in the Configuring RPL Policies in Receiver VRFs to Propagate Joins to a Source VRF: Example, on page 209.

```conf
route-policy extranet_streams_from_provider_rp
  if source in (201.22.22.201) then
    set rpf-topology vrf provider_vrf_1
  else if source in (202.22.22.201) then
    set rpf-topology vrf provider_vrf_2
  else
    pass
endif
end-policy
!
router pim vrf receiver_vrf address-family ipv4
  rp-topology route-policy extranet_streams_from_provider_rp
  rp-address 201.22.22.201 grange_227
  rp-address 202.22.22.201 grange_228
!```
Configuring Multicast Hub and Spoke Topology: Example

These examples describe two ways to configure Multicast Hub and Spoke:

Figure 13: Example for CE1 PE1 PE3 CE3
Multicast Hub and Spoke Topology

CE1------------------ PE1 ------------------------------------------------ PE3 ------------------ CE3

CE1, PE1, and PE3 are all on Cisco IOS XR Software, CE3 has Cisco IOS Software in order to configure autorp on VRF interface. For information about configuring the CE router, using Cisco IOS software, see the appropriate Cisco IOS software documentation.

Hub and Spoke Non-Turnaround Configuration: Example

A1-Spoke-3

No turnaround case with bsr and autorp relay

PE1:

vrf A1-Hub-1
address-family ipv4 unicast
import route-target
  1000:10
  1001:10
!
export route-target
  1000:10
!
!
vrf A1-Hub-Tunnel
address-family ipv4 unicast
import route-target
  1000:10
!
!
!
vrf A1-Spoke-Tunnel
address-family ipv4 unicast
import route-target
  1001:10
!
! router pim
  vrf A1-Hub-1
  address-family ipv4
    rpf topology route-policy A1-Hub-Policy
    bsr relay vrf A1-Hub-Tunnel
    bsr candidate-bsr 201.10.10.201 hash-mask-len 30 priority 4
    bsr candidate-rp 201.10.10.201 group-list A1_PE1_RP_grange priority 4 interval 60
    auto-rp relay vrf A1-Hub-Tunnel
! !
!
router pim
  vrf A1-Hub-Tunnel
  address-family ipv4
  !
  !
multicast-routing
  vrf A1-Hub-1
  address-family ipv4
    log-traps
    multipath
    rate-per-route
    interface all enable
    accounting per-prefix
  !
  !
! multicast-routing
  vrf A1-Hub-Tunnel
  address-family ipv4
    mdt data 226.202.1.0/24 threshold 10
    log-traps
    mdt default ipv4 226.202.0.0
    rate-per-route
accounting per-prefix
!
!

! multicast-routing
vrf A1-Spoke-Tunnel
  address-family ipv4
  mdt mtu 2000
  mdt data 226.202.2.0/24 threshold 5
  log-traps
  mdt default ipv4 226.202.0.1
  rate-per-route
  accounting per-prefix
  !
  !

router bgp 1
vrf A1-Hub-1
  rd 1000:1
  address-family ipv4 unicast
    route-target download
    redistribute connected
    redistribute eigrp 20 match internal external metric 1000
  !
  !

router bgp 1
vrf A1-Hub-Tunnel
  rd 1002:1
  address-family ipv4 unicast
    redistribute connected
    !
  

router bgp 1
vrf A1-Spoke-Tunnel
  rd 1002:2
address-family ipv4 unicast
   redistribute connected
!
!
!
route-policy A1-Hub-Policy
   if extcommunity rt matches-any (1000:10) then
      set rpf-topology vrf A1-Hub-Tunnel
   elseif extcommunity rt matches-any (1001:10) then
      set rpf-topology vrf A1-Spoke-Tunnel
   else
      pass
   endif
end-policy
!
route-policy A1-Spoke-Policy
   if extcommunity rt matches-any (1000:10) then
      set rpf-topology vrf A1-Hub-Tunnel
   else
      pass
   endif
end-policy
!

PE3:

vrf A1-Hub-4
address-family ipv4 unicast
import route-target
   1000:10
   1001:10
!
export route-target
   1000:10
!
!
!

vrf A1-Spoke-2
address-family ipv4 unicast
import route-target
1000:10
!
export route-target
 1001:10
!
!
vrf A1-Hub-Tunnel
address-family ipv4 unicast
import route-target
 1000:10
!
!
!
vrf A1-Spoke-Tunnel
address-family ipv4 unicast
import route-target
 1001:10
!
!
!
router pim
vrf A1-Hub-4
address-family ipv4
  rpf topology route-policy A1-Hub-Policy
bsr relay vrf A1-Hub-Tunnel listen
auto-rp relay vrf A1-Hub-Tunnel
!
!
!
router pim
vrf A1-Spoke-2
address-family ipv4
  rpf topology route-policy A1-Spoke-Policy
bsr relay vrf A1-Hub-Tunnel listen
auto-rp relay vrf A1-Hub-4
!
!
!
multicast-routing
vrf A1-Hub-4
  address-family ipv4
  log-traps
  rate-per-route
  interface all enable
  accounting per-prefix
!
!
!
multicast-routing
vrf A1-Spoke-2
  address-family ipv4
  log-traps
  rate-per-route
  interface all enable
  accounting per-prefix
!
!
!
multicast-routing
vrf A1-Hub-Tunnel
  address-family ipv4
    mdt data 226.202.1.0/24 threshold 10
    log-traps
    mdt default ipv4 226.202.0.0
    rate-per-route
    accounting per-prefix
!
!
!
multicast-routing
vrf A1-Spoke-Tunnel
  address-family ipv4
    mdt data 226.202.2.0/24 threshold 5
    log-traps
    mdt default ipv4 226.202.0.1
rate-per-route
accounting per-prefix
!
!
!
router bgp 1
vrf A1-Hub-4
rd 1000:4
address-family ipv4 unicast
route-target download
redistribute connected
redistribute eigrp 4 match internal external metric 1000
!
!
!
router bgp 1
vrf A1-Spoke-2
rd 1001:2
address-family ipv4 unicast
route-target download
redistribute connected
redistribute eigrp 6 match internal external metric 1000
!
!
!
router bgp 1
vrf A1-Hub-Tunnel
rd 1002:1
address-family ipv4 unicast
redistribute connected
!
!
!
router bgp 1
vrf A1-Spoke-Tunnel
rd 1002:2
address-family ipv4 unicast
redistribute connected
!
! route-policy A1-Hub-Policy
   if extcommunity rt matches-any (1000:10) then
      set rpf-topology vrf A1-Hub-Tunnel
   elseif extcommunity rt matches-any (1001:10) then
      set rpf-topology vrf A1-Spoke-Tunnel
   else
      pass
   endif
end-policy
!
route-policy A1-Spoke-Policy
   if extcommunity rt matches-any (1000:10) then
      set rpf-topology vrf A1-Hub-Tunnel
   else
      pass
   endif
end-policy
!

CE1:

vrf A1-Hub-1
   address-family ipv4 unicast
   import route-target
      1000:10
      1001:10
   !
   export route-target
      1000:10
   !
!
multicast-routing
vrf A1-Hub-1
   address-family ipv4
   log-traps
   rate-per-route
Hub and Spoke with Turnaround: Example

Multicast turnaround mandates a 2-interface connection to the hub site.

To configure a CE as a turnaround router, it is connected to its respective PE through two interfaces and each interface is placed in a separate hub site vrf called hub-x-in vrf and hub-x-out vrf. Hub-x-in vrf carries joins that come from the receiver spoke site through the Hub Tunnel and hub-x-out vrf will carry the same joins.
towards the source spoke site through the Spoke Tunnel without violating the four basic rules below. The source spoke sends traffic to the spoke tunnel to hub-x-out which is turned around to the hub-tunnel on the hub-x-in interface.

1. Hub sites sends traffic only to MDTHub.
2. Spoke sites sends traffic only to MDTspoke.
3. Hub sites receives traffic from both tunnels.
4. Spoke sites receives traffic only from MDTHub.

A2-Spoke-1  A2-Hub-2
A2-Spoke-2  A2-Hub-3in
A2-Hub-2out
A2-Spoke-3 (spoke has auto-rp)

**Figure 14: Example for CE1PE1PE2 CE2 Multicast Hub and Spoke Topology with Turnaround**

CE1------------------ PE1 ------------------------------------------------ PE2 ------------------ CE2

Routes exported by hub sites are imported by hub sites and spoke sites. Routes exported by spoke sites are imported by both hub-x-out and hub-x-in and hub site exports spoke routes back into the core by hub VRF route targets. This causes routes originated from one spoke site to be learned by all other spoke sites but with the nexthop of hub-x-out. For example, Spoke2 will see the RPF for Spoke1 reachable with nexthop of A2-Hub-3in. This is the fundamental difference in leaking of routes which helps in achieving turnaround of multicast traffic.

**PE1:**

```conf
vrf A2-Spoke-1
  address-family ipv4 unicast
  import route-target
    4000:1
    4000:2
    4000:3
    4000:4
  !
  export route-target
    4001:1
  !
  !
  vrf A2-Spoke-2
  address-family ipv4 unicast
```
import route-target
  4000:1
  4000:2
  4000:3
  4000:4
!
export route-target
  4001:2
!
!

PE2:

vrf A2-Hub-2
  address-family ipv4 unicast
    import route-target
      4000:1
      4000:2
      4000:3
      4000:4
      4001:1
      4001:2
      4001:3
      4001:4
    !
    export route-target
      4000:2
    !
    !
    !

vrf A2-Hub-3out
  address-family ipv4 unicast
    import route-target
      4000:1
      4000:2
4000:3
4000:4
4001:1 --------à exports the spoke routes into CE2 into vrf default
4001:2 --------à exports the spoke routes into CE2 into vrf default
4001:3 --------à exports the spoke routes into CE2 into vrf default
4001:4 --------à exports the spoke routes into CE2 into vrf default
!
export route-target

4000:4
!
!
!

vrf A2-Hub-3in

address-family ipv4 unicast
import route-target

4000:1
4000:2
4000:3
4000:4
!
export route-target

4000:3--------À selected spoke routes (in the prefix-set below) can be re-exported with
hub route target so other spokes can reach them via A2-Hub-3in
!
!
!
prefix-set A2-Spoke-family
112.31.1.0/24,
112.32.1.0/24,
152.31.1.0/24,
132.30.1.0/24,
102.9.9.102/32,
103.31.103/32,
183.31.1.0/24,
183.32.1.0/24
end-set
!
route-policy A2-Spoke-family
if destination in A2-Spoke-family then
    pass
else
    drop
endif
end-policy

router bgp 1
vrf A2-Hub-3in
    rd 4000:3
    address-family ipv4 unicast
    route-target download
    redistribute connected
!
neighbor 113.113.114.9
    remote-as 12
    address-family ipv4 unicast

route-policy A2-Spoke-family in ------à leaking the selected spoke routes with hub route targets so they can be imported by the spoke sites with RPF A2-Hub-3in.

    route-policy pass-all out
    !
    !
    !
router bgp 1
vrf A2-Hub-3out
    rd 4000:4
    address-family ipv4 unicast
    route-target download
    redistribute connected
    !
    !
    !
router bgp 1
vrf A2-Hub-2
multicast-routing
vrf A2-Hub-2
    address-family ipv4
    log-traps
    rate-per-route
    interface all enable
    accounting per-prefix
!
!
multicast-routing
vrf A2-Hub-3in
    address-family ipv4
    log-traps
    rate-per-route
    interface all enable
    accounting per-prefix
!
!
multicast-routing
vrf A2-Hub-3out
    address-family ipv4
    log-traps
    rate-per-route
    interface all enable
    accounting per-prefix
!
Any CE-PE protocol can be used. In this example, A2-Hub-3out exports all the hub and spoke routes to CE2 through EIGRP.

A2-Hub-3in uses route policy A2-Spoke-family to re-import selected spoke routes into PE2 through BGP.

```
router eigrp 20
vrf A2-Hub-3out
address-family ipv4
default-metric 1000 1 255 1 1500
autonomous-system 20
redistribute bgp 1
interface GigabitEthernet0/1/0/1.13
hold-time 60
```
CE2:

Here A2-Hub-3in and A2-Hub-3out interfaces are in vrf default and not in a hub site vrf.

interface GigabitEthernet0/12/1/0.12
description To PE2 or vrf A2-Hub-3in
ipv4 address 113.113.114.9 255.255.255.252
encapsulation dot1q 3001
!
interface GigabitEthernet0/12/1/0.13
description To PE2 or vrf A2-Hub-3out
ipv4 address 113.113.114.13 255.255.255.252
encapsulation dot1q 3002
!
routerr bgp 12
nsr
bgp graceful-restart
	ridge-family ipv4 unicast
redistribute connected
redistribute eigrp 20
!
neighbor 113.113.114.10
--à this is the A2-Hub-3in neighbor on PE2.
remote-as 1
address-family ipv4 unicast
route-policy pass-all in
route-policy pass-all out
!
!

Configuring LSM based MLDP: Examples

These examples describe multiple profiles to configure MLDP based MVPN:

Rosen MLDP without BGP-Advertisement

vrf 1
  vpn id 1:1
  address-family ipv4 unicast
  import route-target
  1:1
  !
  export route-target
  1:1
  !
  !
  interface Loopback0
  ipv4 address 1.1.1.1 255.255.255.255
  !
  route-policy mldp-1
  set core-tree mldp-default
  end-policy
  !
  routerr ospf 1
  address-family ipv4 unicast
  area 0
  mpls traffic-eng
  !
  routerr bgp 100 mvpn
  address-family ipv4 unicast
  redistribute connected
  !
  !
address-family vpnv4 unicast
!
address-family vpnv6 unicast
!
address-family ipv4 mdt
!
neighbor 5.5.5.5
remote-as 100
update-source Loopback0
address-family ipv4 unicast
!
address-family vpnv4 unicast
!
address-family vpnv6 unicast
!
address-family ipv4 mdt
!
!
vrf 1
rd 1:1
address-family ipv4 unicast
redistribute connected
!
mpls traffic-eng
interface GigabitEthernet0/0/2/0
!
mpls ldp
router-id 1.1.1.1
graceful-restart
mldp
logging internal
!
<all core-facing interfaces>
!
multicast-routing
address-family ipv4
nsf
mdt source Loopback0
interface all enable
accounting per-prefix
!
vrf 1
address-family ipv4
interface all enable
mdt default mldp ipv4 1.1.1.1
accounting per-prefix
!
!
router pim
vrf 1
address-family ipv4
rpf topology route-policy mldp-1
rp-address 10.1.1.1
!
!
Rosen MLDP with BGP Advertisement

vrf 101
vpn id 101:101
address-family ipv4 unicast
import route-target
101:101
!
export route-target
101:101
!
!
interface Loopback0
  ipv4 address 1.1.1.1 255.255.255.255
!
interface Loopback101
  vrf 101
  ipv4 address 10.1.101.1 255.255.255.255
!
route-policy mldp-101
  set core-tree mldp-default
end-policy
!
routing ospf 1
  address-family ipv4 unicast
  area 0
  mpls traffic-eng
  interface Loopback0
!
interface Loopback1
  !
  interface GigabitEthernet0/0/2/0
  !
  interface GigabitEthernet0/3/2/1
  !
  interface GigabitEthernet0/3/2/2
  !

  mpls traffic-eng router-id Loopback0
!
router bgp 100 mvpn
  address-family ipv4 unicast
  redistribute connected
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
  neighbor 5.5.5.5
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
  vrf 101
  rd 101:101
  address-family ipv4 unicast
  redistribute connected
  !
  address-family ipv4 mvpn
  !
  mpls traffic-eng
  interface GigabitEthernet0/0/2/0
  !

  mpls ldp
  router-id 1.1.1.1
  graceful-restart
  mldp
  logging internal
  !
  <all core-facing interfaces>
  !
  multicast-routing
  address-family ipv4
nsf
mdt source Loopback0
interface all enable
accounting per-prefix

router pim
vrf 101
   address-family ipv4
      rpf topology route-policy mldp-101
      vpn-id 101
      rp-address 10.1.101.1

VRF In-band Profile

vrf 250
   address-family ipv4 unicast
      import route-target
      250:250
      export route-target
      250:250

interface Loopback0
   ipv4 address 1.1.1.1 255.255.255.255

route-policy mldp-250
   set core-tree mldp-inband
end-policy

router ospf 1
   address-family ipv4 unicast
   area 0
      mpls traffic-eng
      interface Loopback0
      interface Loopback1
      interface GigabitEthernet0/0/2/0
      interface GigabitEthernet0/3/2/1
      interface GigabitEthernet0/3/2/2
      mpls traffic-eng router-id Loopback0

router bgp 100
   address-family ipv4 unicast
   redistribute connected
   address-family vpnv4 unicast
   address-family vpnv6 unicast
   neighbor 5.5.5.5
      remote-as 100
      update-source Loopback0
      address-family ipv4 unicast
      address-family vpnv4 unicast
      address-family vpnv6 unicast
vrf 250
rd 250:250
address-family ipv4 unicast
    redistribute connected
! address-family ipv4 mvpn
!
mpls traffic-eng
    interface GigabitEthernet0/0/2/0
! mpls ldp
    router-id 1.1.1.1
    graceful-restart
    mldp
    logging internal
! <all core-facing interfaces>
!
multicast-routing
    address-family ipv4
        nsf
        mdt source Loopback0
        interface all enable
        accounting per-prefix
!
 vrf 250
    address-family ipv4
        mdt mldp in-band-signaling
        interface all enable
!
router pim
 vrf 250
    address-family ipv4
        rpf topology route-policy mldp-250
        rp-address 10.1.250.1
!

Partitioned-MDT MP2MP without BGP-AD

vrf 251
    address-family ipv4 unicast
        import route-target
            251:251
        !
        export route-target
            251:251
!
!
interface Loopback0
    ipv4 address 1.1.1.1 255.255.255.255
!
interface Loopback251
    vrf 251
    ipv4 address 10.11.1.1 255.255.255.255
!
    route-policy mldp-251
        set core-tree mldp-partitioned-mp2mp
    end-policy
!
    router ospf 1
    address-family ipv4 unicast
    area 0
    mpls traffic-eng
interface Loopback0
!
interface Loopback1
!
interface GigabitEthernet0/0/2/0
!
interface GigabitEthernet0/3/2/1
!
interface GigabitEthernet0/3/2/2
!
mpls traffic-eng router-id Loopback0
!
router bgp 100
address-family ipv4 unicast
  redistribute connected
!
address-family vpnv4 unicast
!
address-family vpnv6 unicast
!
neighbor 5.5.5.5
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
  
  address-family vpnv4 unicast
  
  address-family vpnv6 unicast
  
  vrf 251
  rd 251:251
  address-family ipv4 unicast
  redistribute connected

mpls traffic-eng
  interface GigabitEthernet0/0/2/0
  
mpls ldp
  router-id 1.1.1.1
  graceful-restart
  mldp
  logging internal
  
  <all core-facing interfaces>

multicast-routing
  address-family ipv4
  nsf
  mdt source Loopback0
  interface all enable
  accounting per-prefix
  
  vrf 251
  address-family ipv4
  mdt partitioned mldp ipv4 mp2mp
  interface all enable

router pim
  vrf 251
  address-family ipv4
  rpf topology route-policy mldp-251
  rp-address 10.11.1.1


Partitioned-MDT MP2MP with BGP-AD

vrf 301
  address-family ipv4 unicast
  import route-target
  301:301
  export route-target
  301:301

interface Loopback0
  ipv4 address 1.1.1.1 255.255.255.255

interface Loopback301
  vrf 301
  ipv4 address 10.11.51.1 255.255.255.255

route-policy mldp-301
  set core-tree mldp-partitioned-mp2mp
  end-policy

router ospf 1
  address-family ipv4 unicast
  area 0
    mpls traffic-eng
    interface Loopback0
    interface Loopback1
    interface GigabitEthernet0/0/2/0
    interface GigabitEthernet0/3/2/1
    interface GigabitEthernet0/3/2/2

    mpls traffic-eng router-id Loopback0

router bgp 100
  address-family ipv4 unicast
  redistribute connected
    address-family vpnv4 unicast
    address-family vpnv6 unicast
    address-family ipv4 mvpn

  neighbor 5.5.5.5
    remote-as 100
    update-source Loopback0
    address-family ipv4 unicast
    address-family vpnv4 unicast
    address-family vpnv6 unicast
    address-family ipv4 mvpn

vrf 301
  rd 301:301
  address-family ipv4 unicast
    redistribute connected
    address-family ipv4 mvpn

mpls traffic-eng
  interface GigabitEthernet0/0/2/0
mpls ldp
  router-id 1.1.1.1
graceful-restart
mpls
  logging internal
  <all core-facing interfaces>

multicast-routing
  address-family ipv4
    mldp
      mdt source Loopback0
      interface all enable
      accounting per-prefix
    vrf 301
      address-family ipv4
        bgp auto-discovery mldp
        mdt partitioned mldp ipv4 mp2mp
        interface all enable
  !
  !
router ospf 1
  address-family ipv4 unicast
  area 0
  mpls traffic-eng
  interface Loopback0
  !
  interface Loopback1
  !
  interface GigabitEthernet0/0/2/0
  !
  interface GigabitEthernet0/3/2/1
  !
  interface GigabitEthernet0/3/2/2

Multidirectional Selective Provider Multicast Service Instance mLDP-P2MP with BGP-Advertisement

vrf 401
  address-family ipv4 unicast
  import route-target
    401:401
  !
  export route-target
    401:401
  !

  interface Loopback0
    ipv4 address 1.1.1.1 255.255.255.255
  !
  interface Loopback401
    vrf 401
    ipv4 address 10.11.151.1 255.255.255.255
  !
  route-policy mldp-401
    set core-tree mldp-partitioned-p2mp
  end-policy

router ospf 1
  address-family ipv4 unicast
  area 0
  mpls traffic-eng
  interface Loopback0
  !
  interface Loopback1
  !
  interface GigabitEthernet0/0/2/0
  !
  interface GigabitEthernet0/3/2/1
  !
  interface GigabitEthernet0/3/2/2
  !
mpls traffic-eng router-id Loopback0

router bgp 100
  address-family ipv4 unicast
    redistribute connected
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
neighbor 5.5.5.5
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
    !
  address-family vpnv4 unicast
    !
  address-family vpnv6 unicast
    !
  address-family ipv4 mvpn
  !

vrf 401
  rd 401:401
  address-family ipv4 unicast
    redistribute connected
    !
  address-family ipv4 mvpn
  !

mpls traffic-eng
  interface GigabitEthernet0/0/2/0
  !

mpls ldp
  router-id 1.1.1.1
  graceful-restart
  mldp
    logging internal
  !
  <all core-facing interfaces>
  !

multicast-routing
  address-family ipv4
    nsf
    mdt source Loopback0
    interface all enable
    accounting per-prefix
    !
  vrf 401
  address-family ipv4
    bgp auto-discovery mldp
    mdt partitioned mldp ipv4 p2mp
    interface all enable
    !

router pim
  vrf 401
  address-family ipv4
    rpf topology route-policy mldp-401
    rp-address 10.11.151.1
  !

Rosen-GRE with BGP-Advertisement

vrf 501
  address-family ipv4 unicast
import route-target 501:501
!
export route-target 501:501
!
!
interface Loopback0
ipv4 address 1.1.1.1 255.255.255.255
!
interface Loopback501
vrf 501
ipv4 address 10.111.1.1 255.255.255.255
!
<no route policy?>
!
vrf 501
rd 501:501
address-family ipv4 unicast
  redistribute connected
!
address-family ipv4 mvpn
!
!
routing ospf 1
address-family ipv4 unicast
area 0
mpls traffic-eng
interface Loopback0
!
interface Loopback1
!
interface GigabitEthernet0/0/2/0
!
interface GigabitEthernet0/3/2/1
!
interface GigabitEthernet0/3/2/2
!
mpls traffic-eng router-id Loopback0
!
routing bgp 100
address-family ipv4 unicast
  redistribute connected
!
address-family vpnv4 unicast
!
address-family vpnv6 unicast
!
address-family ipv4 mvpn
!
neighbor 5.5.5.5
  remote-as 100
  update-source Loopback0
  address-family ipv4 unicast
  !
  address-family vpnv4 unicast
  !
  address-family vpnv6 unicast
  !
  address-family ipv4 mvpn
  !
!
vrf 501
rd 501:501
address-family ipv4 unicast
  redistribute connected
!
address-family ipv4 mvpn
!
mpls traffic-eng
  interface GigabitEthernet0/0/2/0
  !
mls ldp
  router-id 1.1.1.1
  graceful-restart
  mldp
  logging internal
  !
  <all core-facing interfaces>
  !
  multicast-routing
  address-family ipv4
  nsf
  mdt source Loopback0
  interface all enable accounting per-prefix
  !
  vrf 501
  address-family ipv4
  bgp auto-discovery pim
  mdt default ipv4 232.1.1.1
  interface all enable
  !
  router pim
  vrf 501
  address-family ipv4
  rp-address 10.111.1.1
  !

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast command reference document</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference</td>
</tr>
<tr>
<td>Getting started material</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Getting Started Guide</td>
</tr>
<tr>
<td>Modular quality of service command reference document</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Modular Quality of Service Command Reference</td>
</tr>
<tr>
<td>Routing command reference and configuration documents</td>
<td>Cisco ASR 9000 Series Aggregation Services Router Routing Command Reference</td>
</tr>
<tr>
<td></td>
<td>Cisco ASR 9000 Series Aggregation Services Router Routing Configuration Guide</td>
</tr>
<tr>
<td>Information about user groups and task IDs</td>
<td>Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide</td>
</tr>
</tbody>
</table>