

Multicast VPNs on EX9200 Switches

Release
15.1



Modified: 2015-06-04

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Multicast VPNs on EX9200 Switches

15.1

Copyright © 2015, Juniper Networks, Inc.

All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xi
	Documentation and Release Notes	xi
	Supported Platforms	xi
	Using the Examples in This Manual	xi
	Merging a Full Example	xii
	Merging a Snippet	xii
	Documentation Conventions	xiii
	Documentation Feedback	xv
	Requesting Technical Support	xv
	Self-Help Online Tools and Resources	xv
	Opening a Case with JTAC	xvi
Part 1	Overview	
Chapter 1	Understanding Multicast VPNs	3
	MBGP Multicast VPN Sites	3
	Multicast VPN Terminology	4
Chapter 2	Understanding Layer 3 VPNs	5
	Introduction to Configuring Layer 3 VPNs	5
	Layer 3 VPN Platform Support	8
Chapter 3	Supported Standards	9
	Supported Multicast VPN Standards	9
Part 2	Configuring Multicast on Layer 3 VPNs	
Chapter 4	Creating Next Generation MVPN VRF Import and Export Policies	13
	Limiting Routes to Be Advertised by an MVPN VRF Instance	13
	Configuring VRF Route Targets for Routing Instances for an MBGP MVPN	14
	Configuring the Export Target for an MBGP MVPN	15
	Configuring the Import Target for an MBGP MVPN	16
	Configuring the Import Target Receiver and Sender for an MBGP MVPN	16
	Configuring the Import Target Unicast Parameters for an MBGP MVPN	17
Chapter 5	Signaling Provider Tunnels in Next Generation MVPNs	19
	PIM Sparse Mode, PIM Dense Mode, Auto-RP, and BSR for MBGP MVPNs	19
	Example: Configuring PIM Join Load Balancing On Next-Generation Multicast VPN	20
	Example: Configuring MBGP Multicast VPNs	28

Chapter 6	Distributing Next Generation MVPN Routes	47
	Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs	47
	Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs	49
	Configuring Internet Multicast Using Ingress Replication Provider Tunnels	51
	Example: Configuring PIM State Limits	54
	Controlling PIM Resources for Multicast VPNs Overview	54
	System Log Messages for PIM Resources	56
	Example: Configuring PIM State Limits	57
	Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN	67
	About S-PMSI	67
	Scenarios for Using Wildcard S-PMSI	68
	Types of Wildcard S-PMSI	69
	Differences Between Wildcard S-PMSI and (S,G) S-PMSI	69
	Wildcard (*) S-PMSI and PIM Dense Mode	69
	Wildcard (*) S-PMSI and PIM-BSR	70
	Wildcard Source and the 0.0.0.0/0 Source Prefix	70
	Configuring a Selective Provider Tunnel Using Wildcards	72
	Example: Configuring Selective Provider Tunnels Using Wildcards	73
	Configuring NLRI Parameters for an MBGP MVPN	74
	Configuring Routing Instances for an MBGP MVPN	75
	Configuring Point-to-Multipoint LSPs for an MBGP MVPN	76
	Configuring RSVP-Signaled Inclusive Point-to-Multipoint LSPs for an MBGP MVPN	77
	Configuring Selective Provider Tunnels for an MBGP MVPN	78
	Configuring the Multicast Group Address for an MBGP MVPN	79
	Configuring the Multicast Source Address for an MBGP MVPN	80
	Configuring Static Selective Point-to-Multipoint LSPs for an MBGP MVPN	80
	Configuring Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN	80
	Configuring the Threshold for Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN	81
	Configuring the Tunnel Limit for Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN	81
	Configuring PIM Provider Tunnels for an MBGP MVPN	82
	Configuring PIM-SSM GRE Selective Provider Tunnels	82
Chapter 7	Configuring Draft Rosen VPNs	85
	Example: Configuring PIM Join Load Balancing on Draft-Rosen Multicast VPN	85
Chapter 8	Configuring GRE Tunnel Interfaces for Layer 3 VPNs	95
	Configuring GRE Tunnels for Layer 3 VPNs	95
	Configuring GRE Tunnels Manually Between PE and CE Routers	96
	Configuring the GRE Tunnel Interface on the PE Router	96
	Configuring the GRE Tunnel Interface on the CE Router	97
	Configuring GRE Tunnels Dynamically	97

Part 3	Troubleshooting	
Chapter 9	Tracing Operations	101
	Tracing MBGP MVPN Traffic and Operations	101
Part 4	Configuration Statements and Operational Commands	
Chapter 10	Configuration Statements	105
	[edit protocols bgp] Hierarchy Level	106
	Common BGP Family Options	106
	Complete [edit protocols bgp] Hierarchy	107
	Layer 2 Routing Instances Configuration Hierarchy	113
	advertise-from-main-vpn-tables	116
	create-new-ucast-tunnel	117
	export-target	118
	family (VRF Advertisement)	118
	group (Routing Instances)	119
	group-range (MBGP MVPN Tunnel)	120
	group-rp-mapping	121
	import-target	122
	inet-mvpn (BGP)	123
	inet-mvpn (VRF Advertisement)	124
	inet6-mvpn (BGP)	124
	inet6-mvpn (VRF Advertisement)	125
	ingress-replication	126
	interface (Virtual Tunnel in Routing Instances)	127
	label-switched-path-template (Multicast)	128
	mpls-internet-multicast	129
	multicast (Virtual Tunnel in Routing Instances)	129
	mvpn (NG-MVPN)	130
	mvpn-mode	132
	pim-asm	132
	pim-ssm (Selective Tunnel)	133
	primary (Virtual Tunnel in Routing Instances)	134
	provider-tunnel	135
	register-limit	138
	route-target (Protocols MVPN)	139
	rpt-spt	140
	rsvp-te (Routing Instances Provider Tunnel Selective)	141
	selective	142
	sglimit	144
	source (Routing Instances Provider Tunnel Selective)	145
	spt-only	146
	static-lsp	146
	target (Routing Instances MVPN)	147
	threshold-rate	148
	traceoptions (Protocols MVPN)	149
	tunnel-limit (Routing Instances Provider Tunnel Selective)	151
	unicast (Route Target Community)	152

	unicast (Virtual Tunnel in Routing Instances)	152
	vrf-advertise-selective	153
	wildcard-group-inet	154
	wildcard-group-inet6	155
	wildcard-source (Selective Provider Tunnels)	156
Chapter 11	Operational Commands	157
	Operational-Mode Commands	157
	Overview of Junos OS CLI Operational Mode Commands	157
	CLI Command Categories	157
	Commonly Used Operational Mode Commands	158
	Example: Running Operational Mode Commands on Logical Systems	160
	Example: Viewing BGP Trace Files on Logical Systems	161
	Example: Configuring System Logging on Logical Systems	166

List of Figures

Part 2	Configuring Multicast on Layer 3 VPNs	
Chapter 5	Signaling Provider Tunnels in Next Generation MVPNs	19
	Figure 1: PIM Join Load Balancing on Next-Generation MVPN	23
	Figure 2: Multicast Over Layer 3 VPN Example Topology	29
Chapter 6	Distributing Next Generation MVPN Routes	47
	Figure 3: Internet Multicast Topology	52
	Figure 4: PIM State Limits Topology	58
	Figure 5: Simple MVPN Topology	68
Chapter 7	Configuring Draft Rosen VPNs	85
	Figure 6: PIM Join Load Balancing on Draft-Rosen MVPN	89
Chapter 8	Configuring GRE Tunnel Interfaces for Layer 3 VPNs	95
	Figure 7: GRE Tunnel Configured Between the Local CE Router and the PE Router	95
	Figure 8: GRE Tunnel Configured Between the Remote CE Router and the PE Router	95

List of Tables

	About the Documentation	xi
	Table 1: Notice Icons	xiii
	Table 2: Text and Syntax Conventions	xiii
Part 2	Configuring Multicast on Layer 3 VPNs	
Chapter 6	Distributing Next Generation MVPN Routes	47
	Table 3: PIM System Log Messages	56
Part 4	Configuration Statements and Operational Commands	
Chapter 11	Operational Commands	157
	Table 4: Commonly Used Operational Mode Commands	158

About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Using the Examples in This Manual on page xi
- Documentation Conventions on page xiii
- Documentation Feedback on page xv
- Requesting Technical Support on page xv

Documentation and Release Notes

To obtain the most current version of all Juniper Networks[®] technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- EX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xiii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xiii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<pre>user@host> show chassis alarms</pre> <p>No alarms currently active</p>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	<p>Configure the machine's domain name:</p> <pre>[edit] root@# set system domain-name domain-name</pre>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (string1 string2 string3)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop address; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>

- Download the latest versions of software and review release notes:
<http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Overview

- [Understanding Multicast VPNs on page 3](#)
- [Understanding Layer 3 VPNs on page 5](#)
- [Supported Standards on page 9](#)

CHAPTER 1

Understanding Multicast VPNs

- [MBGP Multicast VPN Sites on page 3](#)
- [Multicast VPN Terminology on page 4](#)

MBGP Multicast VPN Sites

The main characteristics of MBGP MVPNs are:

- They extend Layer 3 VPN service (RFC 4364) to support IP multicast for Layer 3 VPN service providers.
- They follow the same architecture as specified by RFC 4364 for unicast VPNs. Specifically, BGP is used as the provider edge (PE) router-to-PE router control plane for multicast VPN.
- They eliminate the requirement for the virtual router (VR) model (as specified in Internet draft draft-rosen-vpn-mcast, *Multicast in MPLS/BGP VPNs*) for multicast VPNs and the RFC 4364 model for unicast VPNs.
- They rely on RFC 4364-based unicast with extensions for intra-AS and inter-AS communication.

An MBGP MVPN defines two types of site sets, a sender site set and a receiver site set. These sites have the following properties:

- Hosts within the sender site set can originate multicast traffic for receivers in the receiver site set.
- Receivers outside the receiver site set should not be able to receive this traffic.
- Hosts within the receiver site set can receive multicast traffic originated by any host in the sender site set.
- Hosts within the receiver site set should not be able to receive multicast traffic originated by any host that is not in the sender site set.

A site can be in both the sender site set and the receiver site set, so hosts within such a site can both originate and receive multicast traffic. For example, the sender site set could be the same as the receiver site set, in which case all sites could both originate and receive multicast traffic from one another.

Sites within a given MBGP MVPN might be within the same organization or in different organizations, which means that an MBGP MVPN can be either an intranet or an extranet. A given site can be in more than one MBGP MVPN, so MBGP MVPNs might overlap. Not all sites of a given MBGP MVPN have to be connected to the same service provider, meaning that an MBGP MVPN can span multiple service providers. Feature parity for the MVPN extranet functionality or overlapping MVPNs on the Junos Trio chipset is supported in Junos OS Releases 11.1R2, 11.2R2, and 11.4.

Another way to look at an MBGP MVPN is to say that an MBGP MVPN is defined by a set of administrative policies. These policies determine both the sender site set and the receiver site set. These policies are established by MBGP MVPN customers, but implemented by service providers using the existing BGP and MPLS VPN infrastructure.

- Related Documentation**
- *Example: Allowing MBGP MVPN Remote Sources*
 - *Example: Configuring a PIM-SSM Provider Tunnel for an MBGP MVPN*

Multicast VPN Terminology

I

- Inclusive tree** A single multicast distribution tree in the backbone that carries all the multicast traffic from a specified set of one or more multicast VPNs. An inclusive tree that carries the traffic of more than one multicast VPN is an aggregate inclusive tree. An inclusive tree contains as its members all the PE routers that attach to the receiver sites of any of the multicast VPNs using the tree.

S

- Selective tree** A single multicast distribution tree in the backbone that carries traffic belonging only to a specified set of one or more multicast groups, from one or more multicast VPNs. An aggregate selective tree carries traffic for multicast groups that belong to different multicast VPNs. By default, traffic from most multicast groups could be carried by an inclusive tree, whereas traffic from high-bandwidth groups should be carried by a selective tree.

CHAPTER 2

Understanding Layer 3 VPNs

- [Introduction to Configuring Layer 3 VPNs on page 5](#)
- [Layer 3 VPN Platform Support on page 8](#)

Introduction to Configuring Layer 3 VPNs

To configure Layer 3 virtual private network (VPN) functionality, you must enable VPN support on the provider edge (PE) router. You must also configure any provider (P) routers that service the VPN, and you must configure the customer edge (CE) routers so that their routes are distributed into the VPN.

To configure Layer 3 VPNs, you include the following statements:

```
description text;  
instance-type vrf;  
interface interface-name;  
protocols {  
  bgp {  
    group group-name {  
      peer-as as-number;  
      neighbor ip-address;  
    }  
    multihop tth-value;  
  }  
  (ospf | ospf3) {  
    area area {  
      interface interface-name;  
    }  
    domain-id domain-id;  
    domain-vpn-tag number;  
    sham-link {  
      local address;  
    }  
    sham-link-remote address <metric number>;  
  }  
  rip {  
    rip-configuration;  
  }  
}  
route-distinguisher (as-number:id | ip-address:id);  
router-id address;
```

```
routing-options {
  autonomous-system autonomous-system {
    independent-domain;
    loops number;
  }
  forwarding-table {
    export [ policy-names ];
  }
  interface-routes {
    rib-group group-name;
  }
  martians {
    destination-prefix match-type <allow>;
  }
  maximum-paths {
    path-limit;
    log-interval interval;
    log-only;
    threshold percentage;
  }
  maximum-prefixes {
    prefix-limit;
    log-interval interval;
    log-only;
    threshold percentage;
  }
  multipath {
    vpn-unequal-cost;
  }
  options {
    syslog (level level | upto level);
  }
  rib routing-table-name {
    martians {
      destination-prefix match-type <allow>;
    }
    multipath {
      vpn-unequal-cost;
    }
    static {
      defaults {
        static-options;
      }
      route destination-prefix {
        next-hop [ next-hops ];
        static-options;
      }
    }
  }
}
static {
  defaults {
    static-options;
  }
  route destination-prefix {
    policy [ policy-names ];
  }
}
```

```

        static-options;
    }
}
vrf-advertise-selective {
    family {
        inet-mvpn;
        inet6-mvpn;
    }
}
vrf-export [ policy-names ];
vrf-import [ policy-names ];
vrf-target (community | export community-name | import community-name);
vrf-table-label;

```

You can include these statements at the following hierarchy levels:

- **[edit routing-instances *routing-instance-name*]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]**

For Layer 3 VPNs, only some of the statements in the **[edit routing-instances]** hierarchy are valid. For the full hierarchy, see the *Junos OS Routing Protocols Library for Routing Devices*.

In addition to these statements, you must enable a signaling protocol, IBGP sessions between the PE routers, and an interior gateway protocol (IGP) on the PE and P routers.

By default, Layer 3 VPNs are disabled.

Many of the configuration procedures for Layer 3 VPNs are common to all types of VPNs.

Related Documentation

- *Centralized Internet Access Through Layer 3 VPNs*
- *Configuring Hub-and-Spoke VPN Topologies: One Interface*
- *Configuring Hub-and-Spoke VPN Topologies: Two Interfaces*
- *Configuring Overlapping VPNs Using Automatic Route Export*
- *Configuring Overlapping VPNs Using Routing Table Groups*
- *Configuring a Full-Mesh VPN Topology with Route Reflectors*
- *Configuring a GRE Tunnel Interface Between PE Routers*
- *Configuring a GRE Tunnel Interface Between a PE and CE Router*
- *Configuring a Simple Full-Mesh VPN Topology*
- *Configuring an Application-Based Layer 3 VPN Topology*
- *Configuring an ES Tunnel Interface Between a PE and CE Router*
- *Configuring an LDP-over-RSVP VPN Topology*
- *Configuring an OSPF Domain ID for a Layer 3 VPN*
- *Distributed Internet Access Through Layer 3 VPNs*
- *Routing Internet Traffic Through a Separate NAT Device*

- *Routing VPN and Internet Traffic Through Different Interfaces for Layer 3 VPNs*
- *Routing VPN and Internet Traffic Through the Same Interface Bidirectionally (VPN Has Private Addresses)*
- *Routing VPN and Internet Traffic Through the Same Interface Bidirectionally (VPN Has Public Addresses)*
- *Routing VPN and Outgoing Internet Traffic Through the Same Interface and Routing Return Internet Traffic Through a Different Interface*
- *Setting the Forwarding Class of the Ping Packets*

Layer 3 VPN Platform Support

Layer 3 VPNs are supported on most combinations of Juniper Networks routing and switching platforms and PICs capable of running the JUNOS Software.

MX Series routers configured to be in Ethernet services mode can support some of the Junos OS Layer 3 VPN features. For Layer 3 VPNs, Ethernet services mode supports configuring a loopback interface for a VPN routing and forwarding (VRF) instance. You can configure up to two VRF instances in Ethernet services mode. Each VRF instance can handle up to 10,000 routes. The **ping mpls l3vpn** operational mode command is also supported.

CHAPTER 3

Supported Standards

- [Supported Multicast VPN Standards on page 9](#)

Supported Multicast VPN Standards

Junos OS substantially supports the following RFCs and Internet draft, which define standards for multicast virtual private networks (VPNs).

- RFC 6513, *Multicast in MPLS/BGP IP VPNs*
- RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs*
- RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPN*
- RFC 6625, *Wildcards in Multicast VPN Auto-Discovery Routes*
- Internet draft draft-morin-l3vpn-mvpn-fast-failover-06.txt, *Multicast VPN Fast Upstream Failover*
- Internet draft draft-raggarwa-l3vpn-bgp-mvpn-extranet-08.txt, *Extranet in BGP Multicast VPN (MVPN)*

Related Documentation

- [Supported Carrier-of-Carriers and Interprovider VPN Standards](#)
- [Supported VPWS Standards](#)
- [Supported Layer 2 VPN Standards](#)
- [Supported Layer 3 VPN Standards](#)
- [Supported VPLS Standards](#)
- [Supported MPLS Standards](#)
- [Supported Standards for BGP](#)
- [Accessing Standards Documents on the Internet](#)

PART 2

Configuring Multicast on Layer 3 VPNs

- [Creating Next Generation MVPN VRF Import and Export Policies on page 13](#)
- [Signaling Provider Tunnels in Next Generation MVPNs on page 19](#)
- [Distributing Next Generation MVPN Routes on page 47](#)
- [Configuring Draft Rosen VPNs on page 85](#)
- [Configuring GRE Tunnel Interfaces for Layer 3 VPNs on page 95](#)

Creating Next Generation MVPN VRF Import and Export Policies

- [Limiting Routes to Be Advertised by an MVPN VRF Instance on page 13](#)
- [Configuring VRF Route Targets for Routing Instances for an MBGP MVPN on page 14](#)

Limiting Routes to Be Advertised by an MVPN VRF Instance

If a hub-and-spoke deployment uses one VPN routing and forwarding (VRF) routing instance for unicast routing and a separate VRF for MVPN routing, you need to limit the PE routers at the hub site to advertise only IPv4 MVPN routes, only IPv6 MVPN routes, or both. This is necessary to prevent the multicast VRF instance from advertising unicast VPN routes to other PE routers.



NOTE: This configuration does not prevent the exportation of VPN routes to other VRF instances on the same router if the **auto-export** statement is included in the **[edit routing-options]** hierarchy.

To configure a VRF routing instance with the name **green** to advertise MVPN routes from both the **inet** and **inet6** address families, perform the following steps:

1. Configure the VRF routing instance to advertise IPv4 routes.

```
user@host# set routing-instances green vrf-advertise-selective family inet-mvpn
```

2. Configure the VRF routing instance to advertise IPv6 routes.

```
user@host# set routing-instances green vrf-advertise-selective family inet6-mvpn
```

After the configuration is committed, only the MVPN routes for the specified address families are advertised from the VRF instance to remote PE routers. To remove the restriction on routes being advertised, delete the **vrf-advertise-selective** statement.



NOTE: You cannot include the `vrf-advertise-selective` statement and the `no-vrf-advertise` statement in the same VRF configuration. However, if you configure the `vrf-advertise-selective` statement without any of its options, the router has the same behavior as if you configured the `no-vrf-advertise` statement. VPN routes are prevented from being advertised from a VRF routing instance to the remote PE routers.

**Related
Documentation**

- [family on page 118](#)
- [inet-mvpn on page 124](#)
- [inet6-mvpn on page 125](#)
- `no-vrf-advertise`
- [vrf-advertise-selective on page 153](#)

Configuring VRF Route Targets for Routing Instances for an MBGP MVPN

By default, the VPN routing and forwarding (VRF) import and export route targets (configured either using VRF import and export policies or using the **vrf-target** statement) are used for importing and exporting routes with the MBGP MVPN network layer reachability information (NLRI).

You can use the **export-target** and **import-target** statements to override the default VRF import and export route targets. Export and import targets can also be specified specifically for sender sites or receiver sites, or can be borrowed from a configured unicast route target. Note that a sender site export route target is always advertised when security association routes are exported.



NOTE: When you configure an MBGP MVPN routing instance, you should not configure a target value for an MBGP MVPN specific route target that is identical to a target value for a unicast route target configured in another routing instance.

Specifying route targets in the MBGP MVPN NLRI for sender and receiver sites is useful when there is a mix of sender only, receiver only, and sender and receiver sites. A sender site route target is used for exporting automatic discovery routes by a sender site and for importing automatic discovery routes by a receiver site. A receiver site route target is used for exporting routes by a receiver site and importing routes by a sender site. A sender and receiver site exports and imports routes with both route targets.

A provider edge (PE) router with sites in a specific MBGP MVPN must determine whether a received automatic discovery route is from a sender site or receiver site based on the following:

- If the PE router is configured to be only in a sender site, route targets are imported only from receiver sites. Imported automatic discovery routes must be from a receiver site.

- If the PE router is configured to be only in a receiver site, route targets are imported only from sender sites. Imported automatic discovery routes must be from a sender site.
- If a PE router is configured to be in both sender sites and receiver sites, these guidelines apply:
 - Along with an import route target, you can optionally configure whether the route target is from a receiver or a sender site.
 - If a configuration is not provided, an imported automatic discovery route is treated as belonging to both the sender site set and the receiver site set.

To configure a route target for the MBGP MVPN routing instance, include the **route-target** statement:

```
route-target {
  export-target {
    target target-community;
    unicast;
  }
  import-target {
    target {
      target-value;
      receiver target-value;
      sender target-value;
    }
    unicast {
      receiver;
      sender;
    }
  }
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols mvpn]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mvpn]

The following sections describes how to configure the export target and the import target for an MBGP MVPN:

- [Configuring the Export Target for an MBGP MVPN on page 15](#)
- [Configuring the Import Target for an MBGP MVPN on page 16](#)

Configuring the Export Target for an MBGP MVPN

To configure an export target, include the **export-target** statement:

```
export-target {
  target target-community;
  unicast;
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols mvpn route-target]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mvpn route target]

Configure the **target** option to specify the export target community. Configure the **unicast** option to use the same target community that has been specified for unicast.

Configuring the Import Target for an MBGP MVPN

To configure an import target, include the **import-target** statement:

```
import-target {  
  target target-value {  
    receiver;  
    sender;  
  }  
  unicast {  
    receiver;  
    sender;  
  }  
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols mvpn route-target]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mvpn route-target]

The following sections describe how to configure the import target and unicast parameters:

- [Configuring the Import Target Receiver and Sender for an MBGP MVPN on page 16](#)
- [Configuring the Import Target Unicast Parameters for an MBGP MVPN on page 17](#)

Configuring the Import Target Receiver and Sender for an MBGP MVPN

To configure the import target community, include the **target** statement and specify the target community. The target community must be in the format **target:x:y**. The **x** value is either an IP address or an AS number followed by an optional **L** to indicate a 4 byte AS number, and **y** is a number (for example, **target:123456L:100**)

```
target target-value {  
  receiver;  
  sender;  
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols mvpn route-target import-target]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mvpn route-target import-target]

You can specify the target community used when importing either receiver site sets or sender site sets by including one of the following statements:

- **receiver**—Specify the target community used when importing receiver site sets.
- **sender**—Specify the target community used when importing sender site sets.

Configuring the Import Target Unicast Parameters for an MBGP MVPN

To configure a unicast target community as the import target, include the **unicast** statement:

```
unicast {  
    receiver;  
    sender;  
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols mvpn route-target import-target]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols mvpn route-target import-target]

You can specify the unicast target community used when importing either receiver site sets or sender site sets by including one of the following statements:

- **receiver**—Specify the unicast target community used when importing receiver site sets.
- **sender**—Specify the unicast target community used when importing sender site sets.

CHAPTER 5

Signaling Provider Tunnels in Next Generation MVPNs

- [PIM Sparse Mode, PIM Dense Mode, Auto-RP, and BSR for MBGP MVPNs on page 19](#)
- [Example: Configuring PIM Join Load Balancing On Next-Generation Multicast VPN on page 20](#)
- [Example: Configuring MBGP Multicast VPNs on page 28](#)

PIM Sparse Mode, PIM Dense Mode, Auto-RP, and BSR for MBGP MVPNs

You can configure PIM sparse mode, PIM dense mode, auto-RP, and bootstrap router (BSR) for MBGP MVPN networks:

- **PIM sparse mode**—Allows a router to use any unicast routing protocol and performs reverse-path forwarding (RPF) checks using the unicast routing table. PIM sparse mode includes an explicit join message, so routers determine where the interested receivers are and send join messages upstream to their neighbors, building trees from the receivers to the rendezvous point (RP).
- **PIM dense mode**—Allows a router to use any unicast routing protocol and performs reverse-path forwarding (RPF) checks using the unicast routing table. Packets are forwarded to all interfaces except the incoming interface. Unlike PIM sparse mode, where explicit joins are required for packets to be transmitted downstream, packets are flooded to all routers in the routing instance in PIM dense mode.
- **Auto-RP**—Uses PIM dense mode to propagate control messages and establish RP mapping. You can configure an auto-RP node in one of three different modes: discovery mode, announce mode, and mapping mode.
- **BSR**—Establishes RPs. A selected router in a network acts as a BSR, which selects a unique RP for different group ranges. BSR messages are flooded using a data tunnel between PE routers.

Related Documentation

- [Example: Allowing MBGP MVPN Remote Sources](#)
- [Example: Configuring a PIM-SSM Provider Tunnel for an MBGP MVPN](#)

Example: Configuring PIM Join Load Balancing On Next-Generation Multicast VPN

This example shows how to configure multipath routing for external and internal virtual private network (VPN) routes with unequal interior gateway protocol (IGP) metrics and Protocol Independent Multicast (PIM) join load balancing on provider edge (PE) routers running next-generation multicast VPN (MVPN). This feature allows customer PIM (C-PIM) join messages to be load-balanced across available internal BGP (IBGP) upstream paths when there is no external BGP (EBGP) path present, and across available EBGP upstream paths when external and internal BGP (EIBGP) paths are present toward the source or rendezvous point (RP).

- [Requirements on page 20](#)
- [Overview and Topology on page 20](#)
- [Configuration on page 23](#)
- [Verification on page 27](#)

Requirements

This example uses the following hardware and software components:

- Three routers that can be a combination of M Series, MX Series, or T Series routers.
- Junos OS Release 12.1 running on all the devices.

Before you begin:

1. Configure the device interfaces.
2. Configure the following routing protocols on all PE routers:
 - OSPF
 - MPLS
 - LDP
 - PIM
 - BGP
3. Configure a multicast VPN.

Overview and Topology

Junos OS Release 12.1 and later support multipath configuration along with PIM join load balancing. This allows C-PIM join messages to be load-balanced across all available IBGP paths when there are only IBGP paths present, and across all available upstream EBGP paths when EIBGP paths are present toward the source (or RP). Unlike Draft-Rosen MVPN, next-generation MVPN does not utilize unequal EIBGP paths to send C-PIM join messages. This feature is applicable to IPv4 C-PIM join messages.

By default, only one active IBGP path is used to send the C-PIM join messages for a PE router having only IBGP paths toward the source (or RP). When there are EIBGP upstream paths present, only one active EBGp path is used to send the join messages.

In a next-generation MVPN, C-PIM join messages are translated into (or encoded as) BGP customer multicast (C-multicast) MVPN routes and advertised with the BGP MCAST-VPN address family toward the sender PE routers. A PE router originates a C-multicast MVPN route in response to receiving a C-PIM join message through its PE router to customer edge (CE) router interface. The two types of C-multicast MVPN routes are:

- Shared tree join route (C-*, C-G)
 - Originated by receiver PE routers.
 - Originated when a PE router receives a shared tree C-PIM join message through its PE-CE router interface.
- Source tree join route (C-S, C-G)
 - Originated by receiver PE routers.
 - Originated when a PE router receives a source tree C-PIM join message (C-S, C-G), or originated by the PE router that already has a shared tree join route and receives a source active autodiscovery route.

The upstream path in a next-generation MVPN is selected using the Bitwise-XOR hash algorithm as specified in Internet draft draft-ietf-l3vpn-2547bis-mcast, *Multicast in MPLS/BGP IP VPNs*. The hash algorithm is performed as follows:

1. The PE routers in the candidate set are numbered from lower to higher IP address, starting from **0**.
2. A bitwise exclusive-or of all the bytes is performed on the C-root (source) and the C-G (group) address.
3. The result is taken modulo n , where n is the number of PE routers in the candidate set. The result is **N**.
4. **N** represents the IP address of the upstream PE router as numbered in Step 1.

During load balancing, if a PE router with one or more upstream IBGP paths toward the source (or RP) discovers a new IBGP path toward the same source (or RP), the C-PIM join messages distributed among previously existing IBGP paths get redistributed due to the change in the candidate PE router set.

In this example, PE1, PE2, and PE3 are the PE routers that have the multipath PIM join load-balancing feature configured. Router PE1 has two EBGp paths and one IBGP upstream path, PE2 has one EBGp path and one IBGP upstream path, and PE3 has two IBGP upstream paths toward the Source. Router CE4 is the customer edge (CE) router attached to PE3. Source and Receiver are the Free BSD hosts.

On PE routers that have EIBGP paths toward the source (or RP), such as PE1 and PE2, PIM join load balancing is performed as follows:

1. The C-PIM join messages are sent using EIBGP paths only. IBGP paths are not used to propagate the join messages.

In [Figure 1 on page 23](#), the PE1 router distributes the join messages between the two EIBGP paths to the CE1 router, and PE2 uses the EIBGP path to CE1 to send the join messages.

2. If a PE router loses one or more EIBGP paths toward the source (or RP), the RPF neighbor on the multicast tunnel interface is selected based on a hash mechanism.

On discovering the first EIBGP path, only new join messages get load-balanced across available EIBGP paths, whereas the existing join messages on the multicast tunnel interface are not redistributed.

If the EIBGP path from the PE2 router to the CE1 router goes down, PE2 sends the join messages to PE1 using the IBGP path. When the EIBGP path to CE1 is restored, only new join messages that arrive on PE2 use the restored EIBGP path, whereas join messages already sent on the IBGP path are not redistributed.

On PE routers that have only IBGP paths toward the source (or RP), such as the PE3 router, PIM join load balancing is performed as follows:

1. The C-PIM join messages from CE routers get load-balanced only as BGP C-multicast data messages among IBGP paths.

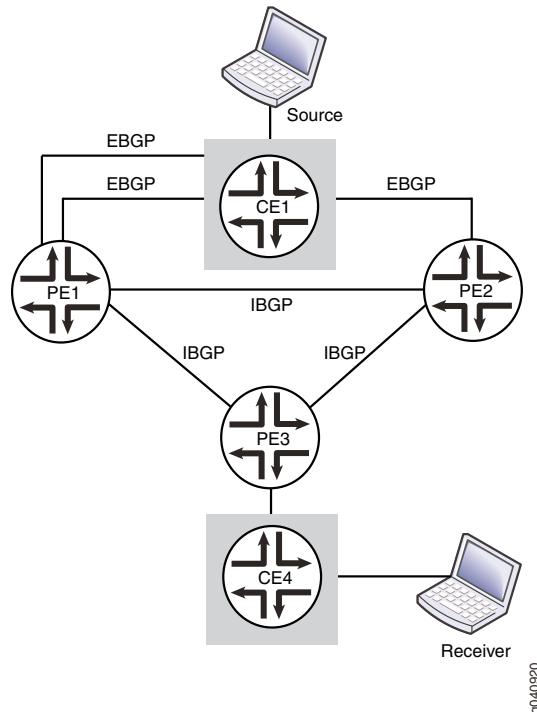
In [Figure 1 on page 23](#), assuming that the CE4 host is interested in receiving traffic from the Source, and CE4 initiates source join messages for different groups (Group 1 [C-S,C-G1] and Group 2 [C-S,C-G2]), the source join messages arrive on the PE3 router.

Router PE3 then uses the Bitwise-XOR hash algorithm to select the upstream PE router to send the C-multicast data for each group. The algorithm first numbers the upstream PE routers from lower to higher IP address starting from 0.

Assuming that Router PE1 router is numbered 0 and Router PE2 is 1, and the hash result for Group 1 and Group 2 join messages is 0 and 1, respectively, the PE3 router selects PE1 as the upstream PE router to send Group 1 join messages, and PE2 as the upstream PE router to send the Group 2 join messages to the Source.

2. The shared join messages for different groups [C-*,C-G] are also treated in a similar way to reach the destination.

Figure 1: PIM Join Load Balancing on Next-Generation MVPN



Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```

PE1 set routing-instances vpn1 instance-type vrf
    set routing-instances vpn1 interface ge-3/0/1.0
    set routing-instances vpn1 interface ge-3/3/2.0
    set routing-instances vpn1 interface lo0.1
    set routing-instances vpn1 route-distinguisher 1:1
    set routing-instances vpn1 provider-tunnel rsvp-te label-switched-path-template
        default-template
    set routing-instances vpn1 vrf-target target:1:1
    set routing-instances vpn1 vrf-table-label
    set routing-instances vpn1 routing-options multipath vpn-unequal-cost
        equal-external-internal
    set routing-instances vpn1 protocols bgp export direct
    set routing-instances vpn1 protocols bgp group bgp type external
    set routing-instances vpn1 protocols bgp group bgp local-address 10.40.10.1
    set routing-instances vpn1 protocols bgp group bgp family inet unicast
    set routing-instances vpn1 protocols bgp group bgp neighbor 10.40.10.2 peer-as 3
    set routing-instances vpn1 protocols bgp group bgp1 type external
    set routing-instances vpn1 protocols bgp group bgp1 local-address 10.10.10.1
    set routing-instances vpn1 protocols bgp group bgp1 family inet unicast
  
```

```
set routing-instances vpn1 protocols bgp group bgp1 neighbor 10.10.10.2 peer-as 3
set routing-instances vpn1 protocols pim rp static address 10.255.10.119
set routing-instances vpn1 protocols pim interface all
set routing-instances vpn1 protocols pim join-load-balance
set routing-instances vpn1 protocols mvpn mvpn-mode rpt-spt
set routing-instances vpn1 protocols mvpn mvpn-join-load-balance bitwise-xor-hash
```

```
PE2 set routing-instances vpn1 instance-type vrf
set routing-instances vpn1 interface ge-1/0/9.0
set routing-instances vpn1 interface lo0.1
set routing-instances vpn1 route-distinguisher 2:2
set routing-instances vpn1 provider-tunnel rsvp-te label-switched-path-template
    default-template
set routing-instances vpn1 vrf-target target:1:1
set routing-instances vpn1 vrf-table-label
set routing-instances vpn1 routing-options multipath vpn-unequal-cost
    equal-external-internal
set routing-instances vpn1 protocols bgp export direct
set routing-instances vpn1 protocols bgp group bgp local-address 10.50.10.2
set routing-instances vpn1 protocols bgp group bgp family inet unicast
set routing-instances vpn1 protocols bgp group bgp neighbor 10.50.10.1 peer-as 3
set routing-instances vpn1 protocols pim rp static address 10.255.10.119
set routing-instances vpn1 protocols pim interface all
set routing-instances vpn1 protocols mvpn mvpn-mode rpt-spt
set routing-instances vpn1 protocols mvpn mvpn-join-load-balance bitwise-xor-hash
```

```
PE3 set routing-instances vpn1 instance-type vrf
set routing-instances vpn1 interface ge-0/0/8.0
set routing-instances vpn1 interface lo0.1
set routing-instances vpn1 route-distinguisher 3:3
set routing-instances vpn1 provider-tunnel rsvp-te label-switched-path-template
    default-template
set routing-instances vpn1 vrf-target target:1:1
set routing-instances vpn1 vrf-table-label
set routing-instances vpn1 routing-options multipath vpn-unequal-cost
    equal-external-internal
set routing-instances vpn1 routing-options autonomous-system 1
set routing-instances vpn1 protocols bgp export direct
set routing-instances vpn1 protocols bgp group bgp type external
set routing-instances vpn1 protocols bgp group bgp local-address 10.80.10.1
set routing-instances vpn1 protocols bgp group bgp family inet unicast
set routing-instances vpn1 protocols bgp group bgp neighbor 10.80.10.2 peer-as 2
set routing-instances vpn1 protocols pim rp static address 10.255.10.119
set routing-instances vpn1 protocols pim interface all
set routing-instances vpn1 protocols mvpn mvpn-mode rpt-spt
set routing-instances vpn1 protocols mvpn mvpn-join-load-balance bitwise-xor-hash
```


Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*. To configure the PE1 router:



NOTE: Repeat this procedure for every Juniper Networks router in the MVPN domain, after modifying the appropriate interface names, addresses, and any other parameters for each router.

1. Configure a VPN routing forwarding (VRF) routing instance.


```
[edit routing-instances vpn1]
user@PE1# set instance-type vrf
user@PE1# set interface ge-3/0/1.0
user@PE1# set interface ge-3/3/2.0
user@PE1# set interface lo0.1
user@PE1# set route-distinguisher 1:1
user@PE1# set provider-tunnel rsvp-te label-switched-path-template
default-template
user@PE1# set vrf-target target:1:1
user@PE1# set vrf-table-label
```
2. Enable protocol-independent load balancing for the VRF instance.


```
[edit routing-instances vpn1]
user@PE1# set routing-options multipath vpn-unequal-cost equal-external-internal
```
3. Configure BGP groups and neighbors to enable PE to CE routing.


```
[edit routing-instances vpn1 protocols]
user@PE1# set bgp export direct
user@PE1# set bgp group bgp type external
user@PE1# set bgp group bgp local-address 10.40.10.1
user@PE1# set bgp group bgp family inet unicast
user@PE1# set bgp group bgp neighbor 10.40.10.2 peer-as 3
user@PE1# set bgp group bgp1 type external
user@PE1# set bgp group bgp1 local-address 10.10.10.1
user@PE1# set bgp group bgp1 family inet unicast
user@PE1# set bgp group bgp1 neighbor 10.10.10.2 peer-as 3
```
4. Configure PIM to enable PE to CE multicast routing.


```
[edit routing-instances vpn1 protocols]
user@PE1# set pim rp static address 10.255.10.119
```
5. Enable PIM on all network interfaces.


```
[edit routing-instances vpn1 protocols]
user@PE1# set pim interface all
```
6. Enable PIM join load balancing for the VRF instance.


```
[edit routing-instances vpn1 protocols]
user@PE1# set pim join-load-balance
```
7. Configure the mode for C-PIM join messages to use rendezvous-point trees, and switch to the shortest-path tree after the source is known.

```
[edit routing-instances vpn1 protocols]
user@PE1# set mvpn mvpn-mode rpt-spt
```

8. Configure the VRF instance to use the Bytewise-XOR hash algorithm.

```
[edit routing-instances vpn1 protocols]
user@PE1# set mvpn mvpn-join-load-balance bytewise-xor-hash
```

Results

From configuration mode, confirm your configuration by entering the **show routing-instances** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@PE1# show routing-instances
routing-instances {
  vpn1 {
    instance-type vrf;
    interface ge-3/0/1.0;
    interface ge-3/3/2.0;
    interface lo0.1;
    route-distinguisher 1:1;
    provider-tunnel {
      rsvp-te {
        label-switched-path-template {
          default-template;
        }
      }
    }
    vrf-target target:1:1;
    vrf-table-label;
    routing-options {
      multipath {
        vpn-unequal-cost equal-external-internal;
      }
    }
    protocols {
      bgp {
        export direct;
        group bgp {
          type external;
          local-address 10.40.10.1;
          family inet {
            unicast;
          }
          neighbor 10.40.10.2 {
            peer-as 3;
          }
        }
        group bgp1 {
          type external;
          local-address 10.10.10.1;
          family inet {
            unicast;
          }
          neighbor 10.10.10.2 {
```

```

        peer-as 3;
    }
}
pim {
    rp {
        static {
            address 10.255.10.119;
        }
    }
    interface all;
    join-load-balance;
}
mvpn {
    mvpn-mode {
        rpt-spt;
    }
    mvpn-join-load-balance {
        bitwise-xor-hash;
    }
}
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying MVPN C-Multicast Route Information for Different Groups of Join Messages on page 27](#)

Verifying MVPN C-Multicast Route Information for Different Groups of Join Messages

Purpose Verify MVPN C-multicast route information for different groups of join messages received on the PE3 router.

Action From operational mode, run the **show mvpn c-multicast** command.

```

user@PE3> show mvpn c-multicast
MVPN instance:
Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel
Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Family : INET

Instance : vpn1
MVPN Mode : RPT-SPT
C-mcast IPv4 (S:G)          Ptnl          St
0.0.0.0/0:225.1.1.1/32      RSVP-TE P2MP:10.255.10.2, 5834,10.255.10.2
4.4.4.2/32:225.1.1.1/32    RSVP-TE P2MP:10.255.10.2, 5834,10.255.10.2
0.0.0.0/0:225.1.1.2/32      RSVP-TE P2MP:10.255.10.14, 47575,10.255.10.14
4.4.4.2/32:225.1.1.2/32    RSVP-TE P2MP:10.255.10.14, 47575,10.255.10.14

```

Meaning The output shows how the PE3 router has load-balanced the C-multicast data for the different groups.

- For source join messages (S,G):
 - 4.4.4.2/32:225.1.1.1/32 (S,G1) toward the PE1 router (10.255.10.2 is the loopback address of Router PE1).
 - 4.4.4.2/32:225.1.1.2/32 (S,G2) toward the PE2 router (10.255.10.14 is the loopback address of Router PE2).
- For shared join messages (*G):
 - 0.0.0.0/0:225.1.1.1/32 (*G1) toward the PE1 router (10.255.10.2 is the loopback address of Router PE1).
 - 0.0.0.0/0:225.1.1.2/32 (*G2) toward the PE2 router (10.255.10.14 is the loopback address of Router PE2).

Related Documentation

- [PIM Join Load Balancing on Multipath MVPN Routes Overview](#)
- [Example: Configuring PIM Join Load Balancing on Draft-Rosen Multicast VPN on page 85](#)

Example: Configuring MBGP Multicast VPNs

This example provides a step-by-step procedure to configure multicast services across a multiprotocol BGP (MBGP) Layer 3 virtual private network. (also referred to as next-generation Layer 3 multicast VPNs)

- [Requirements on page 28](#)
- [Overview and Topology on page 29](#)
- [Configuration on page 29](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 9.2 or later
- Five M Series, T Series, TX Series, or MX Series Juniper routers
- One host system capable of sending multicast traffic and supporting the Internet Group Management Protocol (IGMP)
- One host system capable of receiving multicast traffic and supporting IGMP

Depending on the devices you are using, you might be required to configure static routes to:

- The multicast sender
- The Fast Ethernet interface to which the sender is connected on the multicast receiver

- The multicast receiver
- The Fast Ethernet interface to which the receiver is connected on the multicast sender

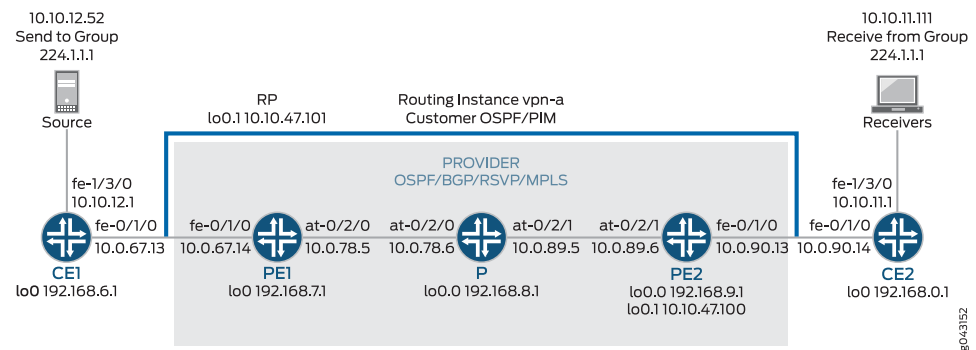
Overview and Topology

This example shows how to configure the following technologies:

- IPv4
- BGP
- OSPF
- RSVP
- MPLS
- PIM sparse mode
- Static RP

The topology of the network is shown in [Figure 2 on page 29](#).

Figure 2: Multicast Over Layer 3 VPN Example Topology



Configuration



NOTE: In any configuration session, it is a good practice to periodically verify that the configuration can be committed using the `commit check` command.

In this example, the router being configured is identified using the following command prompts:

- CE1 identifies the customer edge 1 (CE1) router
- PE1 identifies the provider edge 1 (PE1) router
- P identifies the provider core (P) router

- **CE2** identifies the customer edge 2 (CE2) router
- **PE2** identifies the provider edge 2 (PE2) router

To configure MBGP multicast VPNs for the network shown in [Figure 2 on page 29](#), perform the following steps:

- [Configuring Interfaces on page 30](#)
- [Configuring OSPF on page 31](#)
- [Configuring BGP on page 32](#)
- [Configuring RSVP on page 33](#)
- [Configuring MPLS on page 34](#)
- [Configuring the VRF Routing Instance on page 35](#)
- [Configuring PIM on page 36](#)
- [Configuring the Provider Tunnel on page 36](#)
- [Configuring the Rendezvous Point on page 37](#)
- [Results on page 38](#)

Configuring Interfaces

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. On each router, configure an IP address on the loopback logical interface 0 (**lo0.0**).

```
[edit interfaces]
```

```
user@CE1# set lo0 unit 0 family inet address 192.168.6.1/32 primary
```

```
user@PE1# set lo0 unit 0 family inet address 192.168.7.1/32 primary
```

```
user@P# set lo0 unit 0 family inet address 192.168.8.1/32 primary
```

```
user@PE2# set lo0 unit 0 family inet address 192.168.9.1/32 primary
```

```
user@CE2# set lo0 unit 0 family inet address 192.168.0.1/32 primary
```

Use the **show interfaces terse** command to verify that the IP address is correct on the loopback logical interface.

2. On the PE and CE routers, configure the IP address and protocol family on the Fast Ethernet interfaces. Specify the **inet** protocol family type.

```
[edit interfaces]
```

```
user@CE1# set fe-1/3/0 unit 0 family inet address 10.10.12.1/24
```

```
user@CE1# set fe-0/1/0 unit 0 family inet address 10.0.67.13/30
```

```
[edit interfaces]
```

```
user@PE1# set fe-0/1/0 unit 0 family inet address 10.0.67.14/30
```

```
[edit interfaces]
user@PE2# set fe-0/1/0 unit 0 family inet address 10.0.90.13/30
```

```
[edit interfaces]
user@CE2# set fe-0/1/0 unit 0 family inet address 10.0.90.14/30
user@CE2# set fe-1/3/0 unit 0 family inet address 10.10.11.1/24
```

Use the **show interfaces terse** command to verify that the IP address is correct on the Fast Ethernet interfaces.

3. On the PE and P routers, configure the ATM interfaces' VPI and maximum virtual circuits. If the default PIC type is different on directly connected ATM interfaces, configure the PIC type to be the same. Configure the logical interface VCI, protocol family, local IP address, and destination IP address.

```
[edit interfaces]
user@PE1# set at-0/2/0 atm-options pic-type atm1
user@PE1# set at-0/2/0 atm-options vpi 0 maximum-vcs 256
user@PE1# set at-0/2/0 unit 0 vci 0.128
user@PE1# set at-0/2/0 unit 0 family inet address 10.0.78.5/32 destination 10.0.78.6
```

```
[edit interfaces]
user@P# set at-0/2/0 atm-options pic-type atm1
user@P# set at-0/2/0 atm-options vpi 0 maximum-vcs 256
user@P# set at-0/2/0 unit 0 vci 0.128
user@P# set at-0/2/0 unit 0 family inet address 10.0.78.6/32 destination 10.0.78.5
user@P# set at-0/2/1 atm-options pic-type atm1
user@P# set at-0/2/1 atm-options vpi 0 maximum-vcs 256
user@P# set at-0/2/1 unit 0 vci 0.128
user@P# set at-0/2/1 unit 0 family inet address 10.0.89.5/32 destination 10.0.89.6
```

```
[edit interfaces]
user@PE2# set at-0/2/1 atm-options pic-type atm1
user@PE2# set at-0/2/1 atm-options vpi 0 maximum-vcs 256
user@PE2# set at-0/2/1 unit 0 vci 0.128
user@PE2# set at-0/2/1 unit 0 family inet address 10.0.89.6/32 destination 10.0.89.5
```

Use the **show configuration interfaces** command to verify that the ATM interfaces' VPI and maximum VCs are correct and that the logical interface VCI, protocol family, local IP address, and destination IP address are correct.

Configuring OSPF

Step-by-Step Procedure

1. On the P and PE routers, configure the provider instance of OSPF. Specify the **lo0.0** and ATM core-facing logical interfaces. The provider instance of OSPF on the PE router forms adjacencies with the OSPF neighbors on the other PE router and Router P.

```
user@PE1# set protocols ospf area 0.0.0.0 interface at-0/2/0.0
user@PE1# set protocols ospf area 0.0.0.0 interface lo0.0
```

```
user@P# set protocols ospf area 0.0.0.0 interface lo0.0
user@P# set protocols ospf area 0.0.0.0 interface all
user@P# set protocols ospf area 0.0.0.0 interface fxp0 disable
```

```
user@PE2# set protocols ospf area 0.0.0.0 interface lo0.0
user@PE2# set protocols ospf area 0.0.0.0 interface at-0/2/1.0
```

Use the **show ospf interfaces** command to verify that the **lo0.0** and ATM core-facing logical interfaces are configured for OSPF.

2. On the CE routers, configure the customer instance of OSPF. Specify the loopback and Fast Ethernet logical interfaces. The customer instance of OSPF on the CE routers form adjacencies with the neighbors within the VPN routing instance of OSPF on the PE routers.

```
user@CE1# set protocols ospf area 0.0.0.0 interface fe-0/1/0.0
user@CE1# set protocols ospf area 0.0.0.0 interface fe-1/3/0.0
user@CE1# set protocols ospf area 0.0.0.0 interface lo0.0
```

```
user@CE2# set protocols ospf area 0.0.0.0 interface fe-0/1/0.0
user@CE2# set protocols ospf area 0.0.0.0 interface fe-1/3/0.0
user@CE2# set protocols ospf area 0.0.0.0 interface lo0.0
```

Use the **show ospf interfaces** command to verify that the correct loopback and Fast Ethernet logical interfaces have been added to the OSPF protocol.

3. On the P and PE routers, configure OSPF traffic engineering support for the provider instance of OSPF.

The **shortcuts** statement enables the master instance of OSPF to use a label-switched path as the next hop.

```
user@PE1# set protocols ospf traffic-engineering shortcuts
```

```
user@P# set protocols ospf traffic-engineering shortcuts
```

```
user@PE2# set protocols ospf traffic-engineering shortcuts
```

Use the **show ospf overview** or **show configuration protocols ospf** command to verify that traffic engineering support is enabled.

Configuring BGP

Step-by-Step Procedure

1. On Router P, configure BGP for the VPN. The local address is the local **lo0.0** address. The neighbor addresses are the PE routers' **lo0.0** addresses.

The **unicast** statement enables the router to use BGP to advertise network layer reachability information (NLRI). The **signaling** statement enables the router to use BGP as the signaling protocol for the VPN.

```
user@P# set protocols bgp group group-mvpn type internal
user@P# set protocols bgp group group-mvpn local-address 192.168.8.1
user@P# set protocols bgp group group-mvpn family inet unicast
user@P# set protocols bgp group group-mvpn family inet-mvpn signaling
user@P# set protocols bgp group group-mvpn neighbor 192.168.9.1
user@P# set protocols bgp group group-mvpn neighbor 192.168.7.1
```

Use the **show configuration protocols bgp** command to verify that the router has been configured to use BGP to advertise NLRI.

2. On the PE and P routers, configure the BGP local autonomous system number.

```
user@PE1# set routing-options autonomous-system 0.65010
```

```
user@P# set routing-options autonomous-system 0.65010
```

```
user@PE2# set routing-options autonomous-system 0.65010
```

Use the **show configuration routing-options** command to verify that the BGP local autonomous system number is correct.

3. On the PE routers, configure BGP for the VPN. Configure the local address as the local **lo0.0** address. The neighbor addresses are the **lo0.0** addresses of Router P and the other PE router, PE2.

```
user@PE1# set protocols bgp group group-mvpn type internal
user@PE1# set protocols bgp group group-mvpn local-address 192.168.7.1
user@PE1# set protocols bgp group group-mvpn family inet-vpn unicast
user@PE1# set protocols bgp group group-mvpn family inet-mvpn signaling
user@PE1# set protocols bgp group group-mvpn neighbor 192.168.9.1
user@PE1# set protocols bgp group group-mvpn neighbor 192.168.8.1
```

```
user@PE2# set protocols bgp group group-mvpn type internal
user@PE2# set protocols bgp group group-mvpn local-address 192.168.9.1
user@PE2# set protocols bgp group group-mvpn family inet-vpn unicast
user@PE2# set protocols bgp group group-mvpn family inet-mvpn signaling
user@PE2# set protocols bgp group group-mvpn neighbor 192.168.7.1
user@PE2# set protocols bgp group group-mvpn neighbor 192.168.8.1
```

Use the **show bgp group** command to verify that the BGP configuration is correct.

4. On the PE routers, configure a policy to export the BGP routes into OSPF.

```
user@PE1# set policy-options policy-statement bgp-to-ospf from protocol bgp
user@PE1# set policy-options policy-statement bgp-to-ospf then accept
```

```
user@PE2# set policy-options policy-statement bgp-to-ospf from protocol bgp
user@PE2# set policy-options policy-statement bgp-to-ospf then accept
```

Use the **show policy bgp-to-ospf** command to verify that the policy is correct.

Configuring RSVP

Step-by-Step Procedure

1. On the PE routers, enable RSVP on the interfaces that participate in the LSP. Configure the Fast Ethernet and ATM logical interfaces.

```
user@PE1# set protocols rsvp interface fe-0/1/0.0
user@PE1# set protocols rsvp interface at-0/2/0.0
```

```
user@PE2# set protocols rsvp interface fe-0/1/0.0
user@PE2# set protocols rsvp interface at-0/2/1.0
```

2. On Router P, enable RSVP on the interfaces that participate in the LSP. Configure the ATM logical interfaces.

```
user@P# set protocols rsvp interface at-0/2/0.0
```

```
user@P# set protocols rsvp interface at-0/2/1.0
```

Use the **show configuration protocols rsvp** command to verify that the RSVP configuration is correct.

Configuring MPLS

Step-by-Step Procedure

1. On the PE routers, configure an MPLS LSP to the PE router that is the LSP egress point. Specify the IP address of the **lo0.0** interface on the router at the other end of the LSP. Configure MPLS on the ATM, Fast Ethernet, and **lo0.0** interfaces.

To help identify each LSP when troubleshooting, configure a different LSP name on each PE router. In this example, we use the name **to-pe2** as the name for the LSP configured on PE1 and **to-pe1** as the name for the LSP configured on PE2.

```
user@PE1# set protocols mpls label-switched-path to-pe2 to 192.168.9.1
user@PE1# set protocols mpls interface fe-0/1/0.0
user@PE1# set protocols mpls interface at-0/2/0.0
user@PE1# set protocols mpls interface lo0.0
```

```
user@PE2# set protocols mpls label-switched-path to-pe1 to 192.168.7.1
user@PE2# set protocols mpls interface fe-0/1/0.0
user@PE2# set protocols mpls interface at-0/2/1.0
user@PE2# set protocols mpls interface lo0.0
```

Use the **show configuration protocols mpls** and **show route label-switched-path to-pe1** commands to verify that the MPLS and LSP configuration is correct.

After the configuration is committed, use the **show mpls lsp name to-pe1** and **show mpls lsp name to-pe2** commands to verify that the LSP is operational.

2. On Router P, enable MPLS. Specify the ATM interfaces connected to the PE routers.

```
user@P# set protocols mpls interface at-0/2/0.0
user@P# set protocols mpls interface at-0/2/1.0
```

Use the **show mpls interface** command to verify that MPLS is enabled on the ATM interfaces.

3. On the PE and P routers, configure the protocol family on the ATM interfaces associated with the LSP. Specify the **mpls** protocol family type.

```
user@PE1# set interfaces at-0/2/0 unit 0 family mpls
```

```
user@P# set interfaces at-0/2/0 unit 0 family mpls
user@P# set interfaces at-0/2/1 unit 0 family mpls
```

```
user@PE2# set interfaces at-0/2/1 unit 0 family mpls
```

Use the **show mpls interface** command to verify that the MPLS protocol family is enabled on the ATM interfaces associated with the LSP.

Configuring the VRF Routing Instance

Step-by-Step Procedure

1. On the PE routers, configure a routing instance for the VPN and specify the **vrf** instance type. Add the Fast Ethernet and **lo0.1** customer-facing interfaces. Configure the VPN instance of OSPF and include the BGP-to-OSPF export policy.

```
user@PE1# set routing-instances vpn-a instance-type vrf
user@PE1# set routing-instances vpn-a interface lo0.1
user@PE1# set routing-instances vpn-a interface fe-0/1/0.0
user@PE1# set routing-instances vpn-a protocols ospf export bgp-to-ospf
user@PE1# set routing-instances vpn-a protocols ospf area 0.0.0.0 interface all
```

```
user@PE2# set routing-instances vpn-a instance-type vrf
user@PE2# set routing-instances vpn-a interface lo0.1
user@PE2# set routing-instances vpn-a interface fe-0/1/0.0
user@PE2# set routing-instances vpn-a protocols ospf export bgp-to-ospf
user@PE2# set routing-instances vpn-a protocols ospf area 0.0.0.0 interface all
```

Use the **show configuration routing-instances vpn-a** command to verify that the routing instance configuration is correct.

2. On the PE routers, configure a route distinguisher for the routing instance. A route distinguisher allows the router to distinguish between two identical IP prefixes used as VPN routes. Configure a different route distinguisher on each PE router. This example uses 65010:1 on PE1 and 65010:2 on PE2.

```
user@PE1# set routing-instances vpn-a route-distinguisher 65010:1
```

```
user@PE2# set routing-instances vpn-a route-distinguisher 65010:2
```

Use the **show configuration routing-instances vpn-a** command to verify that the route distinguisher is correct.

3. On the PE routers, configure default VRF import and export policies. Based on this configuration, BGP automatically generates local routes corresponding to the route target referenced in the VRF import policies. This example uses 2:1 as the route target.



NOTE: You must configure the same route target on each PE router for a given VPN routing instance.

```
user@PE1# set routing-instances vpn-a vrf-target target:2:1
```

```
user@PE2# set routing-instances vpn-a vrf-target target:2:1
```

Use the **show configuration routing-instances vpn-a** command to verify that the route target is correct.

4. On the PE routers, configure the VPN routing instance for multicast support.

```
user@PE1# set routing-instances vpn-a protocols mvpn
```

```
user@PE2# set routing-instances vpn-a protocols mvpn
```

Use the **show configuration routing-instance vpn-a** command to verify that the VPN routing instance has been configured for multicast support.

- On the PE routers, configure an IP address on loopback logical interface 1 (**lo0.1**) used in the customer routing instance VPN.

```
user@PE1# set interfaces lo0 unit 1 family inet address 10.10.47.101/32
```

```
user@PE2# set interfaces lo0 unit 1 family inet address 10.10.47.100/32
```

Use the **show interfaces terse** command to verify that the IP address on the loopback interface is correct.

Configuring PIM

Step-by-Step Procedure

- On the PE routers, enable PIM. Configure the **lo0.1** and the customer-facing Fast Ethernet interface. Specify the mode as **sparse** and the version as **2**.

```
user@PE1# set routing-instances vpn-a protocols pim interface lo0.1 mode sparse
user@PE1# set routing-instances vpn-a protocols pim interface lo0.1 version 2
user@PE1# set routing-instances vpn-a protocols pim interface fe-0/1/0.0 mode
sparse
user@PE1# set routing-instances vpn-a protocols pim interface fe-0/1/0.0 version
2
```

```
user@PE2# set routing-instances vpn-a protocols pim interface lo0.1 mode sparse
user@PE2# set routing-instances vpn-a protocols pim interface lo0.1 version 2
user@PE2# set routing-instances vpn-a protocols pim interface fe-0/1/0.0 mode
sparse
user@PE2# set routing-instances vpn-a protocols pim interface fe-0/1/0.0 version
2
```

Use the **show pim interfaces instance vpn-a** command to verify that PIM sparse-mode is enabled on the **lo0.1** interface and the customer-facing Fast Ethernet interface.

- On the CE routers, enable PIM. In this example, we configure all interfaces. Specify the mode as **sparse** and the version as **2**.

```
user@CE1# set protocols pim interface all
```

```
user@CE2# set protocols pim interface all mode sparse
user@CE2# set protocols pim interface all version 2
```

Use the **show pim interfaces** command to verify that PIM sparse mode is enabled on all interfaces.

Configuring the Provider Tunnel

Step-by-Step Procedure

- On Router PE1, configure the provider tunnel. Specify the multicast address to be used.

The **provider-tunnel** statement instructs the router to send multicast traffic across a tunnel.

```
user@PE1# set routing-instances vpn-a provider-tunnel rsvp-te
label-switched-path-template default-template
```

Use the **show configuration routing-instance vpn-a** command to verify that the provider tunnel is configured to use the default LSP template.

2. On Router PE2, configure the provider tunnel. Specify the multicast address to be used.

```
user@PE2# set routing-instances vpn-a provider-tunnel rsvp-te
label-switched-path-template default-template
```

Use the **show configuration routing-instance vpn-a** command to verify that the provider tunnel is configured to use the default LSP template.

Configuring the Rendezvous Point

Step-by-Step Procedure

1. Configure Router PE1 to be the rendezvous point. Specify the **lo0.1** address of Router PE1. Specify the multicast address to be used.

```
user@PE1# set routing-instances vpn-a protocols pim rp local address 10.10.47.101
user@PE1# set routing-instances vpn-a protocols pim rp local group-ranges
224.1.1.1/32
```

Use the **show pim rps instance vpn-a** command to verify that the correct local IP address is configured for the RP.

2. On Router PE2, configure the static rendezvous point. Specify the **lo0.1** address of Router PE1.

```
user@PE2# set routing-instances vpn-a protocols pim rp static address 10.10.47.101
```

Use the **show pim rps instance vpn-a** command to verify that the correct static IP address is configured for the RP.

3. On the CE routers, configure the static rendezvous point. Specify the **lo0.1** address of Router PE1.

```
user@CE1# set protocols pim rp static address 10.10.47.101 version 2
```

```
user@CE2# set protocols pim rp static address 10.10.47.101 version 2
```

Use the **show pim rps** command to verify that the correct static IP address is configured for the RP.

4. Use the **commit check** command to verify that the configuration can be successfully committed. If the configuration passes the check, commit the configuration.
5. Start the multicast sender device connected to CE1.
6. Start the multicast receiver device connected to CE2.
7. Verify that the receiver is receiving the multicast stream.
8. Use **show** commands to verify the routing, VPN, and multicast operation.

Results

The configuration and verification parts of this example have been completed. The following section is for your reference.

The relevant sample configuration for Router CE1 follows.

```
Router CE1 interfaces {
    lo0 {
        unit 0 {
            family inet {
                address 192.168.6.1/32 {
                    primary;
                }
            }
        }
    }
    fe-0/1/0 {
        unit 0 {
            family inet {
                address 10.0.67.13/30;
            }
        }
    }
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 10.10.12.1/24;
            }
        }
    }
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface fe-0/1/0.0;
            interface lo0.0;
            interface fe-1/3/0.0;
        }
    }
    pim {
        rp {
            static {
                address 10.10.47.101 {
                    version 2;
                }
            }
        }
        interface all;
    }
}
```

The relevant sample configuration for Router PE1 follows.

```
Router PE1 interfaces {
    lo0 {
```

```

    unit 0 {
        family inet {
            address 192.168.7.1/32 {
                primary;
            }
        }
    }
}
fe-0/1/0 {
    unit 0 {
        family inet {
            address 10.0.67.14/30;
        }
    }
}
at-0/2/0 {
    atm-options {
        pic-type atm1;
        vpi 0 {
            maximum-vcs 256;
        }
    }
    unit 0 {
        vci 0.128;
        family inet {
            address 10.0.78.5/32 {
                destination 10.0.78.6;
            }
        }
        family mpls;
    }
}
lo0 {
    unit 1 {
        family inet {
            address 10.10.47.101/32;
        }
    }
}
}
routing-options {
    autonomous-system 0.65010;
}
protocols {
    rsvp {
        interface fe-0/1/0.0;
        interface at-0/2/0.0;
    }
    mpls {
        label-switched-path to-pe2 {
            to 192.168.9.1;
        }
        interface fe-0/1/0.0;
        interface at-0/2/0.0;
        interface lo0.0;
    }
}

```

```
bgp {
  group group-mvpn {
    type internal;
    local-address 192.168.7.1;
    family inet-vpn {
      unicast;
    }
    family inet-mvpn {
      signaling;
    }
    neighbor 192.168.9.1;
    neighbor 192.168.8.1;
  }
}
ospf {
  traffic-engineering {
    shortcuts;
  }
  area 0.0.0.0 {
    interface at-0/2/0.0;
    interface lo0.0;
  }
}
policy-options {
  policy-statement bgp-to-ospf {
    from protocol bgp;
    then accept;
  }
}
routing-instances {
  vpn-a {
    instance-type vrf;
    interface lo0.1;
    interface fe-0/1/0.0;
    route-distinguisher 65010:1;
    provider-tunnel {
      rsvp-te {
        label-switched-path-template {
          default-template;
        }
      }
    }
    vrf-target target:2:1;
    protocols {
      ospf {
        export bgp-to-ospf;
        area 0.0.0.0 {
          interface all;
        }
      }
    }
    pim {
      rp {
        local {
          address 10.10.47.101;
          group-ranges {
```



```

        224.1.1.1/32;
    }
}
}
interface lo0.1 {
    mode sparse;
    version 2;
}
interface fe-0/1/0.0 {
    mode sparse;
    version 2;
}
}
}
mvpn;
}
}
}

```

The relevant sample configuration for Router P follows.

```

Router P  interfaces {
            lo0 {
                unit 0 {
                    family inet {
                        address 192.168.8.1/32 {
                            primary;
                        }
                    }
                }
            }
            at-0/2/0 {
                atm-options {
                    pic-type atm1;
                    vpi 0 {
                        maximum-vcs 256;
                    }
                }
                unit 0 {
                    vci 0.128;
                    family inet {
                        address 10.0.78.6/32 {
                            destination 10.0.78.5;
                        }
                    }
                    family mpls;
                }
            }
            at-0/2/1 {
                atm-options {
                    pic-type atm1;
                    vpi 0 {
                        maximum-vcs 256;
                    }
                }
                unit 0 {
                    vci 0.128;

```

```
        family inet {
            address 10.0.89.5/32 {
                destination 10.0.89.6;
            }
        }
        family mpls;
    }
}
routing-options {
    autonomous-system 0.65010;
}
protocols {
    rsvp {
        interface at-0/2/0.0;
        interface at-0/2/1.0;
    }
    mpls {
        interface at-0/2/0.0;
        interface at-0/2/1.0;
    }
    bgp {
        group group-mvpn {
            type internal;
            local-address 192.168.8.1;
            family inet {
                unicast;
            }
            family inet-mvpn {
                signaling;
            }
            neighbor 192.168.9.1;
            neighbor 192.168.7.1;
        }
    }
    ospf {
        traffic-engineering {
            shortcuts;
        }
        area 0.0.0.0 {
            interface lo0.0;
            interface all;
            interface fxp0.0 {
                disable;
            }
        }
    }
}
```

The relevant sample configuration for Router PE2 follows.

```
Router PE2  interfaces {
              lo0 {
                unit 0 {
                  family inet {
                    address 192.168.9.1/32 {
```

```

        primary;
    }
}
}
fe-0/1/0 {
    unit 0 {
        family inet {
            address 10.0.90.13/30;
        }
    }
}
at-0/2/1 {
    atm-options {
        pic-type atm1;
        vpi 0 {
            maximum-vcs 256;
        }
    }
    unit 0 {
        vci 0.128;
        family inet {
            address 10.0.89.6/32 {
                destination 10.0.89.5;
            }
        }
        family mpls;
    }
}
lo0 {
    unit 1 {
        family inet {
            address 10.10.47.100/32;
        }
    }
}
}
routing-options {
    autonomous-system 0.65010;
}
protocols {
    rsvp {
        interface fe-0/1/0.0;
        interface at-0/2/1.0;
    }
    mpls {
        label-switched-path to-pe1 {
            to 192.168.7.1;
        }
        interface lo0.0;
        interface fe-0/1/0.0;
        interface at-0/2/1.0;
    }
    bgp {
        group group-mvpn {
            type internal;

```

```
        local-address 192.168.9.1;
        family inet-vpn {
            unicast;
        }
        family inet-mvpn {
            signaling;
        }
        neighbor 192.168.7.1;
        neighbor 192.168.8.1;
    }
}
ospf {
    traffic-engineering {
        shortcuts;
    }
    area 0.0.0.0 {
        interface lo0.0;
        interface at-0/2/1.0;
    }
}
}
policy-options {
    policy-statement bgp-to-ospf {
        from protocol bgp;
        then accept;
    }
}
routing-instances {
    vpn-a {
        instance-type vrf;
        interface fe-0/1/0.0;
        interface lo0.1;
        route-distinguisher 65010:2;
        provider-tunnel {
            rsvp-te {
                label-switched-path-template {
                    default-template;
                }
            }
        }
    }
}
vrf-target target:2:1;
protocols {
    ospf {
        export bgp-to-ospf;
        area 0.0.0.0 {
            interface all;
        }
    }
    pim {
        rp {
            static {
                address 10.10.47.101;
            }
        }
        interface fe-0/1/0.0 {
            mode sparse;
        }
    }
}
```

```

        version 2;
    }
    interface lo0.1 {
        mode sparse;
        version 2;
    }
}
}
mvpn;
}
}
}

```

The relevant sample configuration for Router CE2 follows.

```

Router CE2 interfaces {
    lo0 {
        unit 0 {
            family inet {
                address 192.168.0.1/32 {
                    primary;
                }
            }
        }
    }
    fe-0/1/0 {
        unit 0 {
            family inet {
                address 10.0.90.14/30;
            }
        }
    }
    fe-1/3/0 {
        unit 0 {
            family inet {
                address 10.10.11.1/24;
            }
            family inet6 {
                address fe80::205:85ff:fe88:ccdb/64;
            }
        }
    }
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface fe-0/1/0.0;
            interface lo0.0;
            interface fe-1/3/0.0;
        }
    }
    pim {
        rp {
            static {
                address 10.10.47.101 {
                    version 2;
                }
            }
        }
    }
}

```

```
    }  
  }  
  interface all {  
    mode sparse;  
    version 2;  
  }  
}
```

**Related
Documentation**

CHAPTER 6

Distributing Next Generation MVPN Routes

- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 47](#)
- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 49](#)
- [Configuring Internet Multicast Using Ingress Replication Provider Tunnels on page 51](#)
- [Example: Configuring PIM State Limits on page 54](#)
- [Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 67](#)
- [Configuring a Selective Provider Tunnel Using Wildcards on page 72](#)
- [Example: Configuring Selective Provider Tunnels Using Wildcards on page 73](#)
- [Configuring NLRI Parameters for an MBGP MVPN on page 74](#)
- [Configuring Routing Instances for an MBGP MVPN on page 75](#)
- [Configuring Point-to-Multipoint LSPs for an MBGP MVPN on page 76](#)
- [Configuring PIM Provider Tunnels for an MBGP MVPN on page 82](#)
- [Configuring PIM-SSM GRE Selective Provider Tunnels on page 82](#)

Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs

For MBGP MVPNs (also referred to as next-generation Layer 3 multicast VPNs), the default mode of operation is shortest path tree only (SPT-only) mode. In SPT-only mode, the active multicast sources are learned through multicast VPN source-active routes. This mode of operation is described in section 14 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt).

In contrast to SPT-only mode, rendezvous point tree (RPT)-SPT mode (also known as shared-tree data distribution) supports the native PIM model of transmitting (*,G) messages from the receiver to the RP for intersite shared-tree join messages.

In SPT-only mode, when a PE router receives a (*, C-G) join message, the router looks for an active source transmitting data to the customer group. If the PE router has a source-active route for the customer group, the router creates a source tree customer multicast route and sends the route to the PE router connected to the VPN site with the source. The source is determined by MVPN's single-forwarder election. When a receiver

sends a (*G) join message in a VPN site, the (*G) join message only travels as far as the PE router. After the join message is converted to a type 6 multicast route, which is equivalent to a (S,G) join message, the route is installed with the no-advertise community setting.



NOTE: The MVPN single-forwarder election follows the rule documented in section 9.1.1 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). The single-forwarder election winner is based on the following rules:

- If the active unicast route to the source is through the interface, then this route is used to determine the upstream multicast hop (UMH).
- If the active unicast route to the source is a VPN route, MVPN selects the UMH based on the highest IP address in the route import community for the VPN routes, and the local master loopback address for local VRF routes.

Single-forwarder election guarantees selection of a unique forwarder for a given customer source (C-S). The upstream PE router might differ for the source tree and the shared tree because the election is based on the customer source and C-RP, respectively. Although the single-forwarder election is sufficient for SPT-only mode, the alternative RPT-SPT mode involves procedures to prevent duplicate traffic from being sent on the shared tree and the source tree. These procedures might require administrator-configured parameters to reduce duplicate traffic and reduce blackholes during RPT to SPT switch and the reverse.

In SPT-only mode, when a source is active, PIM creates a register state for the source both on the DR and on the C-RP (or on a PE router that is running Multicast Source Discovery Protocol [MSDP] between itself and the C-RP). After the register states are created, MVPN creates a source-active route. These type 5 source-active routes are installed on all PE routers. When the egress PE router with the (*G) join message receives the source-active route, it has two routes that it can combine to produce the (S,G) multicast route. The type 6 route informs the PE router that a receiver is interested in group G. The source active route informs the PE router that a source S is transmitting data to group G. MVPN combines this information to produce a multicast join message and advertises this to the ingress PE router, as determined by the single-forwarder election.

For some service providers, the SPT-only implementation is not ideal because it creates a restriction on C-RP configuration. For a PE router to create customer multicast routes from (*,C-G) join messages, the router must learn about active sources through MVPN type 5 source-active routes. These source-active routes can be originated only by a PE router. This means that a PE router in the MVPN must learn about all PIM register messages sent to the RP, which is possible only in the following cases:

- The C-RP is colocated on one of the PEs in the MVPN.
- MSDP is run between the C-RP and the VRF instance on one of the PE routers in the MVPN.

If this restriction is not acceptable, providers can use RPT-SPT mode instead of the default SPT-only mode. However, because SPT-only mode does not transmit (*G) routes between VPN sites, SPT-only mode has the following advantages over RPT-SPT mode:

- Simplified operations by exchanging and processing only source-tree customer multicast routes among PE routers
- Simplified operations by eliminating the need for the service provider to suppress MVPN transient duplicates during the switch from RPT to SPT
- Less control plane overhead in the service provider space by limiting the type of customer multicast routes exchanged, which results in more scalable deployments
- More stable traffic patterns in the backbone without the traffic shifts involved in the RPT-SPT mode
- Easier maintenance in the service provider space due to less state information

To configure SPT-only mode:

1. Explicitly configure SPT-only mode:

```
[edit routing-instances routing-instance-name protocols mvpn mvpn-mode]
user@router# set spt-only
```

2. Include the **spt-only** statement for all VRFs that make up the VPN.

Related Documentation

- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 49](#)
- [Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 67](#)

Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs

For MBGP MVPNs (also referred to as next-generation Layer 3 multicast VPNs), the default mode of operation supports only intersite shortest-path trees (SPTs) for customer PIM (C-PIM) join messages. It does not support rendezvous-point trees (RPTs) for C-PIM join messages. The default mode of operation provides advantages, but it requires either that the customer rendezvous point (C-RP) be located on a PE router or that the Multicast Source Discovery Protocol (MSDP) be used between the C-RP and a PE router so that the PE router can learn about active sources advertised by other PE routers.

If the default mode is not suitable for your environment, you can configure RPT-SPT mode (also known as *shared-tree data distribution*), as documented in section 13 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). RPT-SPT mode supports the native PIM model of transmitting (*G) messages from the receiver to the RP for intersite shared-tree join messages. This means that the type 6 (*G) routes get transmitted from one PE router to another. In RPT-SPT mode, the shared-tree multicast routes are advertised from an egress PE router to the upstream router connected to the VPN site with the C-RP. The single-forwarder election is performed for the C-RP rather

than for the source. The egress PE router takes the upstream hop to advertise the (*,G) and sends the type 6 route toward the upstream PE router. To send the data on the RPT, either inclusive or selective provider tunnels can be used. After the data starts flowing on the RPT, the last-hop router switches to SPT mode, unless you include the **spt-threshold infinity** statements in the configuration.



NOTE: The MVPN single-forwarder election follows the rule documented in section 9.1.1 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt). The single-forwarder election winner is based on the following rules:

- If the active unicast route to the source is through the interface, then this route is used to determine the upstream multicast hop (UMH).
- If the active unicast route to the source is a VPN route, MVPN selects the UMH based on the highest IP address in the route import community for the VPN routes, and the local master loopback address for local VRF routes.

The switch to SPT mode is performed by PIM and not by MVPN type 5 and type 6 routes. After the last-hop router switches to SPT mode, the SPT (S,G) join messages follow the same rules as the SPT-only default mode.

The advantage of RPT-SPT mode is that it provides a method for PE routers to discover sources in the multicast VPN when the C-RP is located on the customer site instead of on a PE router. Because the shared C-tree is established between VPN sites, there is no need to run MSDP between the C-RP and the PE routers. RPT-SPT mode also enables egress PE routers to switch to receiving data from the PE connected to the source after the source information is learned, instead of receiving data from the RP.

In Junos OS Release 15.1 and later, in RPT-SPT mode, PIM SSG Joins are created on the egress PE even if no directly-connected receivers are present.



CAUTION: When you configure RPT-SPT mode, receivers or sources directly attached to the PE router are not supported. As a workaround, place a CE router between any receiver or source and the PE router.

To configure RPT-SPT mode:

1. Enable shared-tree data distribution:

```
[edit routing-instances routing-instance-name protocols mvpn mvpn-mode]
user@router# set rpt-spt
```

2. Include the **rpt-spt** statement for all VRFs that make up the VPN.

Related Documentation

- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 47](#)
- [Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 67](#)

Configuring Internet Multicast Using Ingress Replication Provider Tunnels

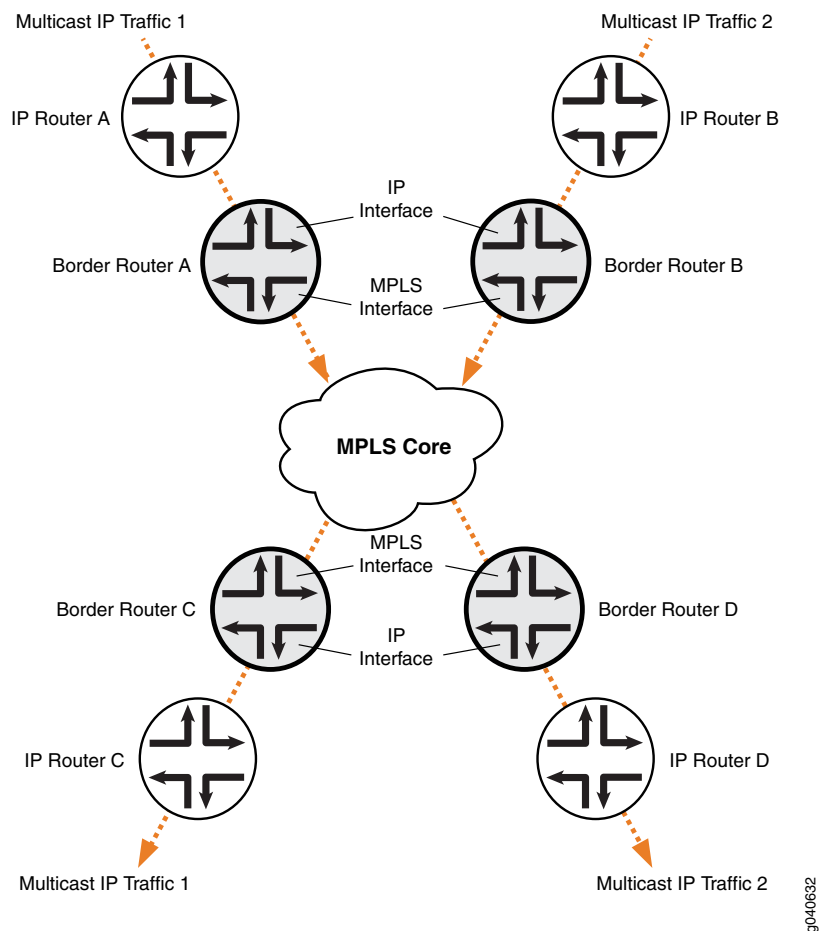
The routing instance type `mpls-internet-multicast` uses ingress replication provider tunnels to carry IP multicast data between routers through an MPLS cloud, enabling a faster path for multicast traffic between sender and receiver routers in large-scale implementations.

The `mpls-internet-multicast` routing instance is a non-forwarding instance used only for control plane procedures; it does not support any interface configurations. Only one `mpls-internet-multicast` routing instance can be defined for a logical system. All multicast and unicast routes used for Internet multicast are associated only with the master instance (`inet.0`), not with the routing instance.

Each router participating in Internet multicast must be configured with BGP MPLS-based Internet multicast for control plane procedures and with ingress replication for the data provider tunnel, which forms a full mesh of MPLS point-to-point LSPs. The ingress replication tunnel can be selective or inclusive, matching the configuration of the provider tunnel in the routing instance.

The topology consists of routers on the edge of the IP multicast domain that have a set of IP interfaces and a set of MPLS core-facing interfaces, see [Figure 3 on page 52](#). Internet multicast traffic is carried between the IP routers, through the MPLS cloud, using ingress replication tunnels for the data plane and a full-mesh IGBP session for the control plane.

Figure 3: Internet Multicast Topology



The `mpls-internet-multicast` routing instance type is configured for the default master instance on each router to support Internet multicast over MPLS. When using PIM as the multicast protocol, the `mpls-internet-multicast` configuration statement is also included at the `[edit protocols pim]` hierarchy level in the master instance. This creates a pseudo-interface that associates PIM with the `mpls-internet-multicast` routing instance.

When a new destination needs to be added to the ingress replication provider tunnel, the resulting behavior differs depending on how the ingress replication provider tunnel is configured:

- **create-new-ucast-tunnel**—When this statement is configured, a new unicast tunnel to the destination is created, and is deleted when the destination is no longer needed. Use this mode for RSVP LSPs using ingress replication.
- **label-switched-path-template (Multicast)**—When this statement is configured, an LSP template is used for the point-to-multipoint LSP for ingress replication.

Example: Configure Internet Multicast Using Ingress Replication Tunnels

This example configures VPN-B with the instance type **mpls-internet-multicast**. This example also uses PIM for the multicast protocol.

1. Configure the routing instance type for VPN-B as **mpls-internet-multicast**:

```
user@host# set routing-instances VPN-B instance-type mpls-internet-multicast
```

2. Configure the ingress replication provider tunnel to create a new unicast tunnel each time an application requests to add a destination:

```
user@host# set routing-instances VPN-B provider-tunnel ingress-replication
create-new-ucast-tunnel
```

3. Configure the point-to-point LSP to use the default template settings.

```
user@host# set routing-instances VPN-B provider-tunnel ingress-replication
label-switched-path label-switched-path-template default-template
```

4. Configure the ingress replication provider tunnel to be selective:

```
user@host# set routing-instances VPN-B provider-tunnel selective group
232.1.1.1/32 source 192.168.195.145/32 ingress-replication label-switched-path
```

5. Configure MVPN protocol in the routing instance:

```
user@host# set routing-instances VPN-B protocols mvpn
```

6. Commit the configuration:

```
user@host# commit
```

7. Use show command to verify the instance has been created:

```
user@host# run show mvpn instance VPN-B
MVPN instance:
Legend for provider tunnel I-P-tnl -- inclusive provider tunnel S-P-tnl --
selective provider tunnel
Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Instance : VPN-B
MVPN Mode : SPT-ONLY
Provider tunnel: I-P-tnl:INGRESS-REPLICATION:MPLS Label 18:10.255.245.6
Neighbor          I-P-tnl
10.255.245.2      INGRESS-REPLICATION:MPLS Label 22:10.255.245.2
10.255.245.7      INGRESS-REPLICATION:MPLS Label 19:10.255.245.7
C-mcast IPv4 (S:G) Ptnl          St
192.168.195.145/32:232.1.1.1/32 INGRESS-REPLICATION:MPLS Label
18:10.255.245.6          RM
```

8. Add the **mpls-internet-multicast** configuration statement under the **[edit protocols pim]** hierarchy level in the master instance:

```
user@host# set protocols pim mpls-internet-multicast
```

9. Commit the configuration:

```
user@host# commit
```

10. Use **show ingress-replication mvpn** command to verify configuration settings:

```
user@host# run show ingress-replication mvpn
Ingress Tunnel: mvpn:11
Application: MVPN
Unicast tunnels
Leaf Address      Tunnel-type      Mode      State
10.255.245.2      P2P LSP         New       Up
10.255.245.4      P2P LSP         New       Up
Ingress Tunnel: mvpn:2
```

Application: MVPN

Unicast tunnels

Leaf Address	Tunnel-type	Mode	State
10.255.245.2	P2P LSP	Existing	Up

11. Use this if you want to configure the ingress replication provider tunnel to be inclusive:

```
user@host# set routing-instances VPN-B provider-tunnel ingress-replication
create-new-ucast-tunnel
user@host# set routing-instances VPN-B provider-tunnel ingress-replication
label-switched-path label-switched-path-template default-template
```

12. Use show myvpn instance command to verify tunnel is inclusive:

```
user@host# run show myvpn instance VPN-B
MVPN instance:
Legend for provider tunnel
I-P-tnl -- inclusive provider tunnel S-P-tnl -- selective provider tunnel

Legend for c-multicast routes properties (Pr)
DS -- derived from (*, c-g)          RM -- remote VPN route
Instance : VPN-A
MVPN Mode : SPT-ONLY
Provider tunnel: I-P-tnl:INGRESS-REPLICATION:MPLS Label 18:10.255.245.6
Neighbor          I-P-tnl
10.255.245.2       INGRESS-REPLICATION:MPLS Label 22:10.255.245.2
10.255.245.7       INGRESS-REPLICATION:MPLS Label 19:10.255.245.7
C-mcast IPv4 (S:G) Ptnl              St
192.168.195.145/32:232.1.1.1/32 INGRESS-REPLICATION:MPLS Label 18:10.255.245.6
RM
```

- Related Documentation
- [create-new-ucast-tunnel on page 117](#)
 - [ingress-replication on page 126](#)
 - [mpls-internet-multicast on page 129](#)

Example: Configuring PIM State Limits

- [Controlling PIM Resources for Multicast VPNs Overview on page 54](#)
- [Example: Configuring PIM State Limits on page 57](#)

Controlling PIM Resources for Multicast VPNs Overview

A service provider network must protect itself from potential attacks from misconfigured or misbehaving customer edge (CE) devices and their associated VPN routing and forwarding (VRF) routing instances. Misbehaving CE devices can potentially advertise a large number of multicast routes toward a provider edge (PE) device, thereby consuming memory on the PE device and using other system resources in the network that are reserved for routes belonging to other VPNs.

To protect against potential misbehaving CE devices and VRF routing instances for specific multicast VPNs (MVPNs), you can control the following Protocol Independent Multicast (PIM) resources:

- Limit the number of accepted PIM join messages for any-source groups (*G) and source-specific groups (S,G).

Note how the device counts the PIM join messages:

- Each (*,G) counts as one group toward the limit.
- Each (S,G) counts as one group toward the limit.
- Limit the number of PIM register messages received for a specific VRF routing instance. Use this configuration if the device is configured as a rendezvous point (RP) or has the potential to become an RP. When a source in a multicast network becomes active, the source's designated router (DR) encapsulates multicast data packets into a PIM register message and sends them by means of unicast to the RP router.

Note how the device counts PIM register messages:

- Each unique (S,G) join received by the RP counts as one group toward the configured register messages limit.
- Periodic register messages sent by the DR for existing or already known (S,G) entries do not count toward the configured register messages limit.
- Register messages are accepted until either the PIM register limit or the PIM join limit (if configured) is exceeded. Once either limit is reached, any new requests are dropped.
- Limit the number of group-to-RP mappings allowed in a specific VRF routing instance. Use this configuration if the device is configured as an RP or has the potential to become an RP. This configuration can apply to devices configured for automatic RP announce and discovery (Auto-RP) or as a PIM bootstrap router. Every multicast device within a PIM domain must be able to map a particular multicast group address to the same RP. Both Auto-RP and the bootstrap router functionality are the mechanisms used to learn the set of group-to-RP mappings. Auto-RP is typically used in a PIM dense-mode deployment, and the bootstrap router is typically used in a PIM sparse-mode deployment.



NOTE: The group-to-RP mappings limit does not apply to static RP or embedded RP configurations.

Some important things to note about how the device counts group-to-RP mappings:

- One group prefix mapped to five RPs counts as five group-to-RP mappings.
- Five distinct group prefixes mapped to one RP count as five group-to-RP mappings.

Once the configured limits are reached, no new PIM join messages, PIM register messages, or group-to-RP mappings are accepted unless one of the following occurs:

- You clear the current PIM join states by using the **clear pim join** command. If you use this command on an RP configured for PIM register message limits, the register limit count is also restarted because the PIM join messages are unknown by the RP.



NOTE: On the RP, you can also use the `clear pim register` command to clear all of the PIM registers. This command is useful if the current PIM register count is greater than the newly configured PIM register limit. After you clear the PIM registers, new PIM register messages are received up to the configured limit.

- The traffic responsible for the excess PIM join messages and PIM register messages stops and is no longer present.



CAUTION: Never restart any of the software processes unless instructed to do so by a customer support engineer.

You restart the PIM routing process on the device. This restart clears all of the configured limits but disrupts routing and therefore requires a maintenance window for the change.

System Log Messages for PIM Resources

You can optionally configure a system log warning threshold for each of the PIM resources. With this configuration, you can generate and review system log messages to detect if an excessive number of PIM join messages, PIM register messages, or group-to-RP mappings have been received on the device. The system log warning thresholds are configured per PIM resource and are a percentage of the configured maximum limits of the PIM join messages, PIM register messages, and group-to-RP mappings. You can further specify a log interval for each configured PIM resource, which is the amount of time (in seconds) between the log messages.

The log messages convey when the configured limits have been exceeded, when the configured warning thresholds have been exceeded, and when the configured limits drop below the configured warning threshold. [Table 3 on page 56](#) describes the different types of PIM system messages that you might see depending on your system log warning and log interval configurations.

Table 3: PIM System Log Messages

System Log Message	Definition
RPD_PIM_SG_THRESHOLD_EXCEED	Records when the (S,G)/(*G) routes exceed the configured warning threshold.
RPD_PIM_REG_THRESH_EXCEED	Records when the PIM registers exceed the configured warning threshold.
RPD_PIM_GRP_RP_MAP_THRES_EXCEED	Records when the group-to-RP mappings exceed the configured warning threshold.
RPD_PIM_SG_LIMIT_EXCEED	Records when the (S,G)/(*G) routes exceed the configured limit, or when the configured log interval has been met and the routes exceed the configured limit.
RPD_PIM_REGISTER_LIMIT_EXCEED	Records when the PIM registers exceed the configured limit, or when the configured log interval has been met and the registers exceed the configured limit.

Table 3: PIM System Log Messages (*continued*)

System Log Message	Definition
RPD_PIM_GRP_RP_MAP_LIMIT_EXCEED	Records when the group-to-RP mappings exceed the configured limit, or when the configured log interval has been met and the mapping exceeds the configured limit.
RPD_PIM_SG_LIMIT_BELOW	Records when the (S,G)/(*G) routes drop below the configured limit and the configured log interval.
RPD_PIM_REGISTER_LIMIT_BELOW	Records when the PIM registers drop below the configured limit and the configured log interval.
RPD_PIM_GRP_RP_MAP_LIMIT_BELOW	Records when the group-to-RP mappings drop below the configured limit and the configured log interval.

Example: Configuring PIM State Limits

This example shows how to set limits on the Protocol Independent Multicast (PIM) state information so that a service provider network can protect itself from potential attacks from misconfigured or misbehaving customer edge (CE) devices and their associated VPN routing and forwarding (VRF) routing instances.

- [Requirements on page 57](#)
- [Overview on page 57](#)
- [Configuration on page 58](#)
- [Verification on page 65](#)

Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

In this example, a multiprotocol BGP-based multicast VPN (next-generation MBGP MVPN) is configured with limits on the PIM state resources.

The **sglimit maximum** statement sets a limit for the number of accepted (*G) and (S,G) PIM join states received for the vpn-l routing instance.

The **rp register-limit maximum** statement configures a limit for the number of PIM register messages received for the vpn-l routing instance. You configure this statement on the rendezvous point (RP) or on all the devices that might become the RP.

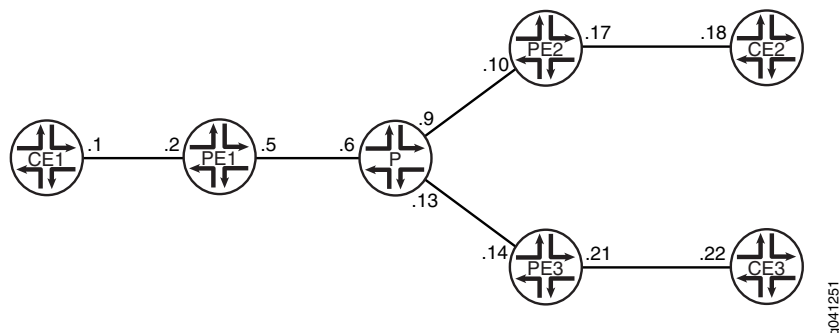
The **group-rp-mapping maximum** statement configures a limit for the number of group-to-RP mappings allowed in the vpn-l routing instance.

For each configured PIM resource, the **threshold** statement sets a percentage of the maximum limit at which to start generating warning messages in the PIM log file.

For each configured PIM resource, the **log-interval** statement is an amount of time (in seconds) between system log message generation.

Figure 4 on page 58 shows the topology used in this example.

Figure 4: PIM State Limits Topology



“CLI Quick Configuration” on page 58 shows the configuration for all of the devices in Figure 4 on page 58. The section “Step-by-Step Procedure” on page 61 describes the steps on Device PE1.

Configuration

CLI Quick Configuration To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

Device CE1

```

set interfaces ge-1/2/0 unit 1 family inet address 10.1.1.1/30
set interfaces ge-1/2/0 unit 1 family mpls
set interfaces lo0 unit 1 family inet address 1.1.1.1/32
set protocols ospf area 0.0.0.0 interface lo0.1 passive
set protocols ospf area 0.0.0.0 interface ge-1/2/0.1
set protocols pim rp static address 100.1.1.2
set protocols pim interface all
set routing-options router-id 1.1.1.1

```

Device PE1

```

set interfaces ge-1/2/0 unit 2 family inet address 10.1.1.2/30
set interfaces ge-1/2/0 unit 2 family mpls
set interfaces ge-1/2/1 unit 5 family inet address 10.1.1.5/30
set interfaces ge-1/2/1 unit 5 family mpls
set interfaces vt-1/2/0 unit 2 family inet
set interfaces lo0 unit 2 family inet address 1.1.1.2/32
set interfaces lo0 unit 102 family inet address 100.1.1.2/32
set protocols mpls interface ge-1/2/1.5
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 1.1.1.2
set protocols bgp group ibgp family inet-vpn any
set protocols bgp group ibgp family inet-mvpn signaling
set protocols bgp group ibgp neighbor 1.1.1.4
set protocols bgp group ibgp neighbor 1.1.1.5
set protocols ospf area 0.0.0.0 interface lo0.2 passive
set protocols ospf area 0.0.0.0 interface ge-1/2/1.5

```

```

set protocols ldp interface ge-1/2/1.5
set protocols ldp p2mp
set policy-options policy-statement parent_vpn_routes from protocol bgp
set policy-options policy-statement parent_vpn_routes then accept
set routing-instances vpn-1 instance-type vrf
set routing-instances vpn-1 interface ge-1/2/0.2
set routing-instances vpn-1 interface vt-1/2/0.2
set routing-instances vpn-1 interface lo0.102
set routing-instances vpn-1 route-distinguisher 100:100
set routing-instances vpn-1 provider-tunnel ldp-p2mp
set routing-instances vpn-1 vrf-target target:1:1
set routing-instances vpn-1 protocols ospf export parent_vpn_routes
set routing-instances vpn-1 protocols ospf area 0.0.0.0 interface lo0.102 passive
set routing-instances vpn-1 protocols ospf area 0.0.0.0 interface ge-1/2/0.2
set routing-instances vpn-1 protocols pim sglimit family inet maximum 100
set routing-instances vpn-1 protocols pim sglimit family inet threshold 70
set routing-instances vpn-1 protocols pim sglimit family inet log-interval 10
set routing-instances vpn-1 protocols pim rp register-limit family inet maximum 100
set routing-instances vpn-1 protocols pim rp register-limit family inet threshold 80
set routing-instances vpn-1 protocols pim rp register-limit family inet log-interval 10
set routing-instances vpn-1 protocols pim rp group-rp-mapping family inet maximum 100
set routing-instances vpn-1 protocols pim rp group-rp-mapping family inet threshold 80
set routing-instances vpn-1 protocols pim rp group-rp-mapping family inet log-interval 10
set routing-instances vpn-1 protocols pim rp static address 100.1.1.2
set routing-instances vpn-1 protocols pim interface ge-1/2/0.2 mode sparse
set routing-instances vpn-1 protocols mvpn
set routing-options router-id 1.1.1.2
set routing-options autonomous-system 1001

```

Device P

```

set interfaces ge-1/2/0 unit 6 family inet address 10.1.1.6/30
set interfaces ge-1/2/0 unit 6 family mpls
set interfaces ge-1/2/1 unit 9 family inet address 10.1.1.9/30
set interfaces ge-1/2/1 unit 9 family mpls
set interfaces ge-1/2/2 unit 13 family inet address 10.1.1.13/30
set interfaces ge-1/2/2 unit 13 family mpls
set interfaces lo0 unit 3 family inet address 1.1.1.3/32
set protocols mpls interface ge-1/2/0.6
set protocols mpls interface ge-1/2/1.9
set protocols mpls interface ge-1/2/2.13
set protocols ospf area 0.0.0.0 interface lo0.3 passive
set protocols ospf area 0.0.0.0 interface ge-1/2/0.6
set protocols ospf area 0.0.0.0 interface ge-1/2/1.9
set protocols ospf area 0.0.0.0 interface ge-1/2/2.13
set protocols ldp interface ge-1/2/0.6
set protocols ldp interface ge-1/2/1.9
set protocols ldp interface ge-1/2/2.13
set protocols ldp p2mp
set routing-options router-id 1.1.1.3

```

Device PE2

```

set interfaces ge-1/2/0 unit 10 family inet address 10.1.1.10/30
set interfaces ge-1/2/0 unit 10 family mpls
set interfaces ge-1/2/1 unit 17 family inet address 10.1.1.17/30
set interfaces ge-1/2/1 unit 17 family mpls
set interfaces vt-1/2/0 unit 4 family inet

```

```

set interfaces lo0 unit 4 family inet address 1.1.1.4/32
set interfaces lo0 unit 104 family inet address 100.1.1.4/32
set protocols mpls interface ge-1/2/0.10
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 1.1.1.4
set protocols bgp group ibgp family inet-vpn any
set protocols bgp group ibgp family inet-mvpn signaling
set protocols bgp group ibgp neighbor 1.1.1.2
set protocols bgp group ibgp neighbor 1.1.1.5
set protocols ospf area 0.0.0.0 interface lo0.4 passive
set protocols ospf area 0.0.0.0 interface ge-1/2/0.10
set protocols ldp interface ge-1/2/0.10
set protocols ldp p2mp
set policy-options policy-statement parent_vpn_routes from protocol bgp
set policy-options policy-statement parent_vpn_routes then accept
set routing-instances vpn-1 instance-type vrf
set routing-instances vpn-1 interface vt-1/2/0.4
set routing-instances vpn-1 interface ge-1/2/1.17
set routing-instances vpn-1 interface lo0.104
set routing-instances vpn-1 route-distinguisher 100:100
set routing-instances vpn-1 vrf-target target:1:1
set routing-instances vpn-1 protocols ospf export parent_vpn_routes
set routing-instances vpn-1 protocols ospf area 0.0.0.0 interface lo0.104 passive
set routing-instances vpn-1 protocols ospf area 0.0.0.0 interface ge-1/2/1.17
set routing-instances vpn-1 protocols pim rp group-rp-mapping family inet maximum 100
set routing-instances vpn-1 protocols pim rp group-rp-mapping family inet threshold 80
set routing-instances vpn-1 protocols pim rp group-rp-mapping family inet log-interval
    10
set routing-instances vpn-1 protocols pim rp static address 100.1.1.2
set routing-instances vpn-1 protocols pim interface ge-1/2/1.17 mode sparse
set routing-instances vpn-1 protocols mvpn
set routing-options router-id 1.1.1.4
set routing-options autonomous-system 1001

```

Device PE3

```

set interfaces ge-1/2/0 unit 14 family inet address 10.1.1.14/30
set interfaces ge-1/2/0 unit 14 family mpls
set interfaces ge-1/2/1 unit 21 family inet address 10.1.1.21/30
set interfaces ge-1/2/1 unit 21 family mpls
set interfaces vt-1/2/0 unit 5 family inet
set interfaces lo0 unit 5 family inet address 1.1.1.5/32
set interfaces lo0 unit 105 family inet address 100.1.1.5/32
set protocols mpls interface ge-1/2/0.14
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 1.1.1.5
set protocols bgp group ibgp family inet-vpn any
set protocols bgp group ibgp family inet-mvpn signaling
set protocols bgp group ibgp neighbor 1.1.1.2
set protocols bgp group ibgp neighbor 1.1.1.4
set protocols ospf area 0.0.0.0 interface lo0.5 passive
set protocols ospf area 0.0.0.0 interface ge-1/2/0.14
set protocols ldp interface ge-1/2/0.14
set protocols ldp p2mp
set policy-options policy-statement parent_vpn_routes from protocol bgp
set policy-options policy-statement parent_vpn_routes then accept
set routing-instances vpn-1 instance-type vrf
set routing-instances vpn-1 interface vt-1/2/0.5

```

```

set routing-instances vpn-1 interface ge-1/2/1.21
set routing-instances vpn-1 interface lo0.105
set routing-instances vpn-1 route-distinguisher 100:100
set routing-instances vpn-1 vrf-target target:1:1
set routing-instances vpn-1 protocols ospf export parent_vpn_routes
set routing-instances vpn-1 protocols ospf area 0.0.0.0 interface lo0.105 passive
set routing-instances vpn-1 protocols ospf area 0.0.0.0 interface ge-1/2/1.21
set routing-instances vpn-1 protocols pim rp static address 100.1.1.2
set routing-instances vpn-1 protocols pim interface ge-1/2/1.21 mode sparse
set routing-instances vpn-1 protocols mvpn
set routing-options router-id 1.1.1.5
set routing-options autonomous-system 1001

```

Device CE2

```

set interfaces ge-1/2/0 unit 18 family inet address 10.1.1.18/30
set interfaces ge-1/2/0 unit 18 family mpls
set interfaces lo0 unit 6 family inet address 1.1.1.6/32
set protocols sap listen 224.1.1.1
set protocols ospf area 0.0.0.0 interface lo0.6 passive
set protocols ospf area 0.0.0.0 interface ge-1/2/0.18
set protocols pim rp static address 100.1.1.2
set protocols pim interface all
set routing-options router-id 1.1.1.6

```

Device CE3

```

set interfaces ge-1/2/0 unit 22 family inet address 10.1.1.22/30
set interfaces ge-1/2/0 unit 22 family mpls
set interfaces lo0 unit 7 family inet address 1.1.1.7/32
set protocols ospf area 0.0.0.0 interface lo0.7 passive
set protocols ospf area 0.0.0.0 interface ge-1/2/0.22
set protocols pim rp static address 100.1.1.2
set protocols pim interface all
set routing-options router-id 1.1.1.7

```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure PIM state limits:

1. Configure the network interfaces.

```

[edit interfaces]
user@PE1# set ge-1/2/0 unit 2 family inet address 10.1.1.2/30
user@PE1# set ge-1/2/0 unit 2 family mpls

```

```

user@PE1# set ge-1/2/1 unit 5 family inet address 10.1.1.5/30
user@PE1# set ge-1/2/1 unit 5 family mpls

```

```

user@PE1# set vt-1/2/0 unit 2 family inet

```

```

user@PE1# set lo0 unit 2 family inet address 1.1.1.2/32
user@PE1# set lo0 unit 102 family inet address 100.1.1.2/32

```

2. Configure MPLS on the core-facing interface.

```

[edit protocols mpls]

```

```
user@PE1# set interface ge-1/2/1.5
```

3. Configure internal BGP (IBGP) on the main router.

The IBGP neighbors are the other PE devices.

```
[edit protocols bgp group ibgp]
user@PE1# set type internal
user@PE1# set local-address 1.1.1.2
user@PE1# set family inet-vpn any
user@PE1# set family inet-mvpn signaling
user@PE1# set neighbor 1.1.1.4
user@PE1# set neighbor 1.1.1.5
```

4. Configure OSPF on the main router.

```
[edit protocols ospf area 0.0.0.0]
user@PE1# set interface lo0.2 passive
user@PE1# set interface ge-1/2/1.5
```

5. Configure a signaling protocol (RSVP or LDP) on the main router.

```
[edit protocols ldp]
user@PE1# set interface ge-1/2/1.5
user@PE1# set p2mp
```

6. Configure the BGP export policy.

```
[edit policy-options policy-statement parent_vpn_routes]
user@PE1# set from protocol bgp
user@PE1# set then accept
```

7. Configure the routing instance.

The customer-facing interfaces and the BGP export policy are referenced in the routing instance.

```
[edit routing-instances vpn-1]
user@PE1# set instance-type vrf
```

```
user@PE1# set interface ge-1/2/0.2
user@PE1# set interface vt-1/2/0.2
user@PE1# set interface lo0.102
```

```
user@PE1# set route-distinguisher 100:100
user@PE1# set provider-tunnel ldp-p2mp
user@PE1# set vrf-target target:1:1
```

```
user@PE1# set protocols ospf export parent_vpn_routes
user@PE1# set protocols ospf area 0.0.0.0 interface lo0.102 passive
user@PE1# set protocols ospf area 0.0.0.0 interface ge-1/2/0.2
```

```
user@PE1# set protocols pim rp static address 100.1.1.2
user@PE1# set protocols pim interface ge-1/2/0.2 mode sparse
```

```
user@PE1# set protocols mvpn
```

8. Configure the PIM state limits.

```
[edit routing-instances vpn-1 protocols pim]
user@PE1# set sglimit family inet maximum 100
user@PE1# set sglimit family inet threshold 70
user@PE1# set sglimit family inet log-interval 10

user@PE1# set rp register-limit family inet maximum 100
user@PE1# set rp register-limit family inet threshold 80
user@PE1# set rp register-limit family inet log-interval 10

user@PE1# set rp group-rp-mapping family inet maximum 100
user@PE1# set rp group-rp-mapping family inet threshold 80
user@PE1# set rp group-rp-mapping family inet log-interval 10
```

9. Configure the router ID and AS number.

```
[edit routing-options]
user@PE1# set router-id 1.1.1.2
user@PE1# set autonomous-system 1001
```

Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show protocols**, **show policy-options**, **show routing-instances**, and **show routing-options** commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@PE1# show interfaces
ge-1/2/0 {
  unit 2 {
    family inet {
      address 10.1.1.2/30;
    }
    family mpls;
  }
}
ge-1/2/1 {
  unit 5 {
    family inet {
      address 10.1.1.5/30;
    }
    family mpls;
  }
}
vt-1/2/0 {
  unit 2 {
    family inet;
  }
}
lo0 {
  unit 2 {
    family inet {
      address 1.1.1.2/32;
    }
  }
  unit 102 {
    family inet {
      address 100.1.1.2/32;
    }
  }
}
```

```
    }
  }
}

user@PE1# show protocols
mpls {
  interface ge-1/2/1.5;
}
bgp {
  group ibgp {
    type internal;
    local-address 1.1.1.2;
    family inet-vpn {
      any;
    }
    family inet-mvpn {
      signaling;
    }
    neighbor 1.1.1.4;
    neighbor 1.1.1.5;
  }
}
ospf {
  area 0.0.0.0 {
    interface lo0.2 {
      passive;
    }
    interface ge-1/2/1.5;
  }
}
ldp {
  interface ge-1/2/1.5;
  p2mp;
}

user@PE1# show policy-options
policy-statement parent_vpn_routes {
  from protocol bgp;
  then accept;
}

user@PE1# show routing-instances
vpn-1 {
  instance-type vrf;
  interface ge-1/2/0.2;
  interface vt-1/2/0.2;
  interface lo0.102;
  route-distinguisher 100:100;
  provider-tunnel {
    ldp-p2mp;
  }
  vrf-target target:1:1;
  protocols {
    ospf {
      export parent_vpn_routes;
      area 0.0.0.0 {
        interface lo0.102 {
```



```

        passive;
    }
    interface ge-1/2/0.2;
}
}
pim {
    sglimit {
        family inet {
            maximum 100;
            threshold 70;
            log-interval 10;
        }
    }
    rp {
        register-limit {
            family inet {
                maximum 100;
                threshold 80;
                log-interval 10;
            }
        }
        group-rp-mapping {
            family inet {
                maximum 100;
                threshold 80;
                log-interval 10;
            }
        }
    }
    static {
        address 100.1.1.2;
    }
}
interface ge-1/2/0.2 {
    mode sparse;
}
}
mvpn;
}

user@PE1# show routing-options
router-id 1.1.1.2;
autonomous-system 1001;

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

Monitoring the PIM State Information

Purpose Verify that the counters are set as expected and are not exceeding the configured limits.

Action From operational mode, enter the **show pim statistics** command.

```
user@PE1> show pim statistics instance vpn-1
PIM Message type      Received      Sent  Rx errors
V2 Hello                393          390         0
...
V4 (S,G) Maximum                100
V4 (S,G) Accepted                0
V4 (S,G) Threshold              70
V4 (S,G) Log Interval           10
V4 (grp-prefix, RP) Maximum     100
V4 (grp-prefix, RP) Accepted     0
V4 (grp-prefix, RP) Threshold   80
V4 (grp-prefix, RP) Log Interval 10
V4 Register Maximum            100
V4 Register Accepted            0
V4 Register Threshold           80
V4 Register Log Interval        10
```

Meaning The V4 (S,G) Maximum field shows the maximum number of (S,G) IPv4 multicast routes accepted for the VPN routing instance. If this number is met, additional (S,G) entries are not accepted.

The V4 (S,G) Accepted field shows the number of accepted (S,G) IPv4 multicast routes.

The V4 (S,G) Threshold field shows the threshold at which a warning message is logged (percentage of the maximum number of (S,G) IPv4 multicast routes accepted by the device).

The V4 (S,G) Log Interval field shows the time (in seconds) between consecutive log messages.

The V4 (grp-prefix, RP) Maximum field shows the maximum number of group-to-rendezvous point (RP) IPv4 multicast mappings accepted for the VRF routing instance. If this number is met, additional mappings are not accepted.

The V4 (grp-prefix, RP) Accepted field shows the number of accepted group-to-RP IPv4 multicast mappings.

The V4 (grp-prefix, RP) Threshold field shows the threshold at which a warning message is logged (percentage of the maximum number of group-to-RP IPv4 multicast mappings accepted by the device).

The V4 (grp-prefix, RP) Log Interval field shows the time (in seconds) between consecutive log messages.

The V4 Register Maximum field shows the maximum number of IPv4 PIM registers accepted for the VRF routing instance. If this number is met, additional PIM registers are not accepted. You configure the register limits on the RP.

The V4 Register Accepted field shows the number of accepted IPv4 PIM registers.

The V4 Register Threshold field shows the threshold at which a warning message is logged (percentage of the maximum number of IPv4 PIM registers accepted by the device).

The V4 Register Log Interval field shows the time (in seconds) between consecutive log messages.

Related Documentation

- [Limiting the Number of IGMP Multicast Group Joins on Logical Interfaces](#)
- [Examples: Configuring the Multicast Forwarding Cache](#)
- [Example: Configuring MSDP with Active Source Limits and Mesh Groups](#)

Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN

Selective LSPs are also referred to as selective provider tunnels. Selective provider tunnels carry traffic from some multicast groups in a VPN and extend only to the PE routers that have receivers for these groups. You can configure a selective provider tunnel for group prefixes and source prefixes, or you can use wildcards for the group and source, as described in the Internet draft draft-rekhter-mvpn-wildcard-spmsi-01.txt, *Use of Wildcard in S-PMSI Auto-Discovery Routes*.

The following sections describe the scenarios and special considerations when you use wildcards for selective provider tunnels.

- [About S-PMSI on page 67](#)
- [Scenarios for Using Wildcard S-PMSI on page 68](#)
- [Types of Wildcard S-PMSI on page 69](#)
- [Differences Between Wildcard S-PMSI and \(S,G\) S-PMSI on page 69](#)
- [Wildcard \(*,*\) S-PMSI and PIM Dense Mode on page 69](#)
- [Wildcard \(*,*\) S-PMSI and PIM-BSR on page 70](#)
- [Wildcard Source and the 0.0.0.0/0 Source Prefix on page 70](#)

About S-PMSI

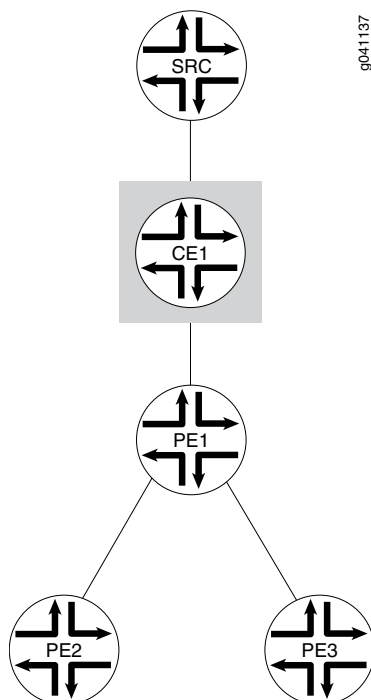
The provider multicast service interface (PMSI) is a BGP tunnel attribute that contains the tunnel ID used by the PE router for transmitting traffic through the core of the provider network. A selective PMSI (S-PMSI) autodiscovery route advertises binding of a given MVPN customer multicast flow to a particular provider tunnel. The S-PMSI autodiscovery route advertised by the ingress PE router contains /32 IPv4 or /128 IPv6 addresses for the customer source and the customer group derived from the source-tree customer multicast route.

[Figure 5 on page 68](#) shows a simple MVPN topology. The ingress router, PE1, originates the S-PMSI autodiscovery route. The egress routers, PE2 and PE3, have join state as a result of receiving join messages from CE devices that are not shown in the topology. In response to the S-PMSI autodiscovery route advertisement sent by PE1, PE2, and PE3, elect whether or not to join the tunnel based on the join state. The selective provider tunnel configuration is configured in a VRF instance on PE1.



NOTE: The MVPN mode configuration (RPT-SPT or SPT-only) is configured on all three PE routers for all VRFs that make up the VPN. If you omit the MVPN mode configuration, the default mode is SPT-only.

Figure 5: Simple MVPN Topology



Scenarios for Using Wildcard S-PMSI

A wildcard S-PMSI has the source or the group (or both the source and the group) field set to the wildcard value of 0.0.0.0/0 and advertises binding of multiple customer multicast flows to a single provider tunnel in a single S-PMSI autodiscovery route.

The scenarios under which you might configure a wildcard S-PMSI are as follows:

- When the customer multicast flows are PIM-SM in ASM-mode flows. In this case, a PE router connected to an MVPN customer's site that contains the customer's RP (C-RP) could bind all the customer multicast flows traveling along a customer's RPT tree to a single provider tunnel.
- When a PE router is connected to an MVPN customer's site that contains multiple sources, all sending to the same group.
- When the customer multicast flows are PIM-bidirectional flows. In this case, a PE router could bind to a single provider tunnel all the customer multicast flows for the same group that have been originated within the sites of a given MVPN connected to that PE, and advertise such binding in a single S-PMSI autodiscovery route.

- When the customer multicast flows are PIM-SM in SSM-mode flows. In this case, a PE router could bind to a single provider tunnel all the customer multicast flows coming from a given source located in a site connected to that PE router.
- When you want to carry in the provider tunnel all the customer multicast flows originated within the sites of a given MVPN connected to a given PE router.

Types of Wildcard S-PMSI

The following types of wildcard S-PMSI are supported:

- A (*,G) S-PMSI matches all customer multicast routes that have the group address. The customer source address in the customer multicast route can be any address, including 0.0.0.0/0 for shared-tree customer multicast routes. A (*, C-G) S-PMSI autodiscovery route is advertised with the source field set to 0 and the source address length set to 0. The multicast group address for the S-PMSI autodiscovery route is derived from the customer multicast joins.
- A (*,*) S-PMSI matches all customer multicast routes. Any customer source address and any customer group address in a customer multicast route can be bound to the (*,*) S-PMSI. The S-PMSI autodiscovery route is advertised with the source address and length set to 0 and the group address and length set 0. The remaining fields in the S-PMSI autodiscovery route follow the same rule as (C-S, C-G) S-PMSI, as described in section 12.1 of the BGP-MVPN draft (draft-ietf-l3vpn-2547bis-mcast-bgp-00.txt).

Differences Between Wildcard S-PMSI and (S,G) S-PMSI

For dynamic provider tunnels, each customer multicast stream is bound to a separate provider tunnel, and each tunnel is advertised by a separate S-PMSI autodiscovery route. For static LSPs, multiple customer multicast flows are bound to a single provider tunnel by having multiple S-PMSI autodiscovery routes advertise the same provider tunnel.

When you configure a wildcard (*,G) or (*,*) S-PMSI, one or more matching customer multicast routes share a single S-PMSI. All customer multicast routes that have a matching source and group address are bound to the same (*,G) or (*,*) S-PMSI and share the same tunnel. The (*,G) or (*,*) S-PMSI is established when the first matching remote customer multicast join message is received in the ingress PE router, and deleted when the last remote customer multicast join is withdrawn from the ingress PE router. Sharing a single S-PMSI autodiscovery route improves control plane scalability.

Wildcard (*,*) S-PMSI and PIM Dense Mode

For (S,G) and (*,G) S-PMSI autodiscovery routes in PIM dense mode (PIM-DM), all downstream PE routers receive PIM-DM traffic. If a downstream PE router does not have receivers that are interested in the group address, the PE router instantiates prune state and stops receiving traffic from the tunnel.

Now consider what happens for (*,*) S-PMSI autodiscovery routes. If the PIM-DM traffic is not bound by a longer matching (S,G) or (*,G) S-PMSI, it is bound to the (*,*) S-PMSI. As is always true for dense mode, PIM-DM traffic is flooded to downstream PE routers over the provider tunnel regardless of the customer multicast join state. Because there is no group information in the (*,*) S-PMSI autodiscovery route, egress PE routers join a

(*,*) S-PMSI tunnel if there is any configuration on the egress PE router indicating interest in PIM-DM traffic.

Interest in PIM-DM traffic is indicated if the egress PE router has one of the following configurations in the VRF instance that corresponds to the instance that imports the S-PMSI autodiscovery route:

- At least one interface is configured in dense mode at the **[edit routing-instances instance-name protocols pim interface]** hierarchy level.
- At least one group is configured as a dense-mode group at the **[edit routing-instances instance-name protocols pim dense-groups group-address]** hierarchy level.

Wildcard (*,*) S-PMSI and PIM-BSR

For (S,G) and (*,G) S-PMSI autodiscovery routes in PIM bootstrap router (PIM-BSR) mode, an ingress PE router floods the PIM bootstrap message (BSM) packets over the provider tunnel to all egress PE routers. An egress PE router does not join the tunnel unless the message has the ALL-PIM-ROUTERS group. If the message has this group, the egress PE router joins the tunnel, regardless of the join state. The group field in the message determines the presence or absence of the ALL-PIM-ROUTERS address.

Now consider what would happen for (*,*) S-PMSI autodiscovery routes used with PIM-BSR mode. If the PIM BSM packets are not bound by a longer matching (S,G) or (*,G) S-PMSI, they are bound to the (*,*) S-PMSI. As is always true for PIM-BSR, BSM packets are flooded to downstream PE routers over the provider tunnel to the ALL-PIM-ROUTERS destination group. Because there is no group information in the (*,*) S-PMSI autodiscovery route, egress PE routers always join a (*,*) S-PMSI tunnel. Unlike PIM-DM, the egress PE routers might have no configuration suggesting use of PIM-BSR as the RP discovery mechanism in the VRF instance. To prevent all egress PE routers from always joining the (*,*) S-PMSI tunnel, the (*,*) wildcard group configuration must be ignored.

This means that if you configure PIM-BSR, a wildcard-group S-PMSI can be configured for all other group addresses. The (*,*) S-PMSI is not used for PIM-BSR traffic. Either a matching (*,G) or (S,G) S-PMSI (where the group address is the ALL-PIM-ROUTERS group) or an inclusive provider tunnel is needed to transmit data over the provider core. For PIM-BSR, the longest-match lookup is (S,G), (*,G), and the inclusive provider tunnel, in that order. If you do not configure an inclusive tunnel for the routing instance, you must configure a (*,G) or (S,G) selective tunnel. Otherwise, the data is dropped. This is because PIM-BSR functions like PIM-DM, in that traffic is flooded to downstream PE routers over the provider tunnel regardless of the customer multicast join state. However, unlike PIM-DM, the egress PE routers might have no configuration to indicate interest or noninterest in PIM-BSR traffic.

Wildcard Source and the 0.0.0.0/0 Source Prefix

You can configure a 0.0.0.0/0 source prefix and a wildcard source under the same group prefix in a selective provider tunnel. For example, the configuration might look as follows:

```
routing-instances {  
  vpna {
```

```

provider-tunnel {
  selective {
    group 224.1.1.0/24 {
      source 0.0.0.0/0 {
        rsvp-te {
          label-switched-path-template {
            sptnl3;
          }
        }
      }
    }
    wildcard-source {
      rsvp-te {
        label-switched-path-template {
          sptnl2;
        }
        static-lsp point-to-multipoint-lsp-name;
      }
      threshold-rate kbps;
    }
  }
}

```

The functions of the **source 0.0.0.0/0** and **wildcard-source** configuration statements are different. The 0.0.0.0/0 source prefix only matches (C-S, C-G) customer multicast join messages and triggers (C-S, C-G) S-PMSI autodiscovery routes derived from the customer multicast address. Because all (C-S, C-G) join messages are matched by the 0.0.0.0/0 source prefix in the matching group, the wildcard source S-PMSI is used only for (*C-G) customer multicast join messages. In the absence of a configured 0.0.0.0/0 source prefix, the wildcard source matches (C-S, C-G) and (*C-G) customer multicast join messages. In the example, a join message for (10.0.1.0/24, 224.1.1.0/24) is bound to **sptnl3**. A join message for (*, 224.1.1.0/24) is bound to **sptnl2**.

Related Documentation

- [Configuring a Selective Provider Tunnel Using Wildcards on page 72](#)
- [Example: Configuring Selective Provider Tunnels Using Wildcards on page 73](#)
- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 47](#)
- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 49](#)

Configuring a Selective Provider Tunnel Using Wildcards

When you configure a selective provider tunnel for MBGP MVPNs (also referred to as next-generation Layer 3 multicast VPNs), you can use wildcards for the multicast group and source address prefixes. Using wildcards enables a PE router to use a single route to advertise the binding of multiple multicast streams of a given MVPN customer to a single provider's tunnel, as described in <http://tools.ietf.org/html/draft-rekhter-mvpn-wildcard-spmsi-00>.

Sharing a single route improves control plane scalability because it reduces the number of S-PMSI autodiscovery routes.

To configure a selective provider tunnel using wildcards:

1. Configure a wildcard group matching any group IPv4 address and a wildcard source for (*,*) join messages.

```
[edit routing-instances vpna provider-tunnel selective]
user@router# set wildcard-group-inet wildcard-source
```

2. Configure a wildcard group matching any group IPv6 address and a wildcard source for (*,*) join messages.

```
[edit routing-instances vpna provider-tunnel selective]
user@router# set wildcard-group-inet6 wildcard-source
```

3. Configure an IP prefix of a multicast group and a wildcard source for (*,G) join messages.

```
[edit routing-instances vpna provider-tunnel selective]
user@router# set group 224.0.0/24 wildcard-source
```

4. Map the IPv4 join messages to a selective provider tunnel.

```
[edit routing-instances vpna provider-tunnel selective wildcard-group-inet
wildcard-source]
user@router# set rsvp-te (Routing Instances Provider Tunnel Selective)
label-switched-path-template provider-tunnel1
```

5. Map the IPv6 join messages to a selective provider tunnel.

```
[edit routing-instances vpna provider-tunnel selective wildcard-group-inet6
wildcard-source]
user@router# set rsvp-te (Routing Instances Provider Tunnel Selective)
label-switched-path-template provider-tunnel2
```

6. Map the (*,224.0.0/24) join messages to a selective provider tunnel.

```
[edit routing-instances vpna provider-tunnel selective group 224.0.0/24
wildcard-source]
user@router# set rsvp-te (Routing Instances Provider Tunnel Selective)
label-switched-path-template provider-tunnel3
```

Related Documentation

- [Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 67](#)
- [Example: Configuring Selective Provider Tunnels Using Wildcards on page 73](#)

- [Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 47](#)
- [Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 49](#)

Example: Configuring Selective Provider Tunnels Using Wildcards

With the (*G) and (**) S-PMSI, a customer multicast join message can match more than one S-PMSI. In this case, a customer multicast join message is bound to the longest matching S-PMSI. The longest match is a (S,G) S-PMSI, followed by a (*G) S-PMSI and a (**) S-PMSI, in that order.

Consider the following configuration:

```
routing-instances {
  vpna {
    provider-tunnel {
      selective {
        wildcard-group-inet {
          wildcard-source {
            rsvp-te {
              label-switched-path-template {
                sptnl1;
              }
            }
          }
        }
      }
    }
    group 224.1.1.0/24 {
      wildcard-source {
        rsvp-te {
          label-switched-path-template {
            sptnl2;
          }
        }
      }
    }
    source 10.1.1/24 {
      rsvp-te {
        label-switched-path-template {
          sptnl3;
        }
      }
    }
  }
}
```

For this configuration, the longest-match rule works as follows:

- A customer multicast (10.1.1.1, 224.1.1.1) join message is bound to the sptnl3 S-PMSI autodiscovery route.

- A customer multicast (10.2.1.1, 224.1.1.1) join message is bound to the sptnl2 S-PMSI autodiscovery route.
- A customer multicast (10.1.1.1, 224.2.1.1) join message is bound to the sptnl1 S-PMSI autodiscovery route.

When more than one customer multicast route is bound to the same wildcard S-PMSI, only one S-PMSI autodiscovery route is created. An egress PE router always uses the same matching rules as the ingress PE router that advertises the S-PMSI autodiscovery route. This ensures consistent customer multicast mapping on the ingress and the egress PE routers.

**Related
Documentation**

- [Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 67](#)
- [Configuring a Selective Provider Tunnel Using Wildcards on page 72](#)

Configuring NLRI Parameters for an MBGP MVPN

To enable VPN signaling where multiprotocol BGP carries multicast VPN NLRI for the IPv4 address family, include the **family inet-mvpn** statement:

```
inet-mvpn {  
  signaling {  
    accepted-prefix-limit {  
      maximum number;  
      teardown percentage {  
        idle-timeout (forever | minutes);  
      }  
    }  
    loops number;  
    prefix-limit {  
      maximum number;  
      teardown percentage {  
        idle-timeout (forever | minutes);  
      }  
    }  
  }  
}
```

To enable VPN signaling where multiprotocol BGP carries multicast VPN NLRI for the IPv6 address family, include the **family inet6-mvpn** statement:

```
inet6-mvpn {  
  signaling {  
    accepted-prefix-limit {  
      maximum number;  
      teardown percentage {  
        idle-timeout (forever | minutes);  
      }  
    }  
    loops number;  
    prefix-limit {  
      maximum number;  
    }  
  }  
}
```

```

        teardown percentage {
            idle-timeout (forever | minutes);
        }
    }
}

```

Configuring Routing Instances for an MBGP MVPN

To configure MBGP MVPNs, include the **mvpn** statement:

```

mvpn {
  mvpn-mode (rpt-spt | spt-only);
  receiver-site;
  route-target {
    export-target {
      target target-community;
      unicast;
    }
    import-target {
      target {
        target-value;
        receiver target-value;
        sender target-value;
      }
      unicast {
        receiver;
        sender;
      }
    }
  }
  sender-site;
  traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
  }
}

```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* protocols]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols]

By default an MBGP MVPN routing instance is associated with both the multicast sender and the receiver sites. If you configure the **receiver-site** option, the routing instance is associated with only multicast receiver sites. Configuring the **sender-site** option associates the routing instance with only multicast sender sites.



NOTE: When you configure the routing instance for the MBGP MVPN, you must configure MPLS LSPs (either RSVP-signaled or LDP-signaled) between the PE routers of the routing instance to ensure VPN unicast connectivity. Point-to-multipoint LSPs are used for multicast data forwarding only.

Configuring Point-to-Multipoint LSPs for an MBGP MVPN

The Junos OS supports point-to-multipoint label-switched paths (LSPs) for MBGP MVPNs. Point-to-multipoint LSPs for multicast VPNs are supported for intra-autonomous system (AS) environments (within an AS), but are not supported for inter-AS environments (between autonomous systems). A point-to-multipoint LSP is an RSVP-signaled LSP with a single source and multiple destinations.

You can configure point-to-multipoint LSPs for MBGP MVPNs as follows:

- Static point-to-multipoint LSPs—Configure static point-to-multipoint LSPs using the standard MPLS LSP statements specified at the **[edit protocols mpls]** hierarchy level. You manually configure each of the leaf nodes for the point-to-multipoint LSP.
- Dynamic point-to-multipoint LSPs using the default template—Configuring dynamic point-to-multipoint LSPs using the **default-template** option causes the leaf nodes to be discovered automatically. The leaf nodes are discovered through BGP intra-AS automatic discovery. The **default-template** option allows you to minimize the amount of configuration needed. However, it does not allow you to configure any of the standard MPLS options.
- Dynamic point-to-multipoint LSPs using a user-configured template—Configuring dynamic point-to-multipoint LSPs using a user-configured template also causes the leaf nodes to be discovered automatically. By creating your own template for the point-to-multipoint LSPs, all of the standard MPLS features (such as bandwidth allocation and traffic engineering) can be configured.

Be aware of the following properties for the egress PE router in a point-to-multipoint LSP configured for a multicast VPN:

- Penultimate hop-popping is not used by point-to-multipoint LSPs for multicast VPNs. Only ultimate hop-popping is used.
- You must configure either the **vrf-table-label** statement or a virtual loopback tunnel interface on the egress PE router.
- If you configure the **vrf-table-label** statement on the egress PE router, and the egress PE router is also a transit router for the point-to-multipoint LSP, the penultimate hop router sends two copies of each packet over the link to the egress PE router.
- If you configure the **vrf-table-label** statement on the egress PE router, and the egress PE router is not a transit router for the point-to-multipoint LSP, the penultimate hop router can send just one copy of each packet over the link to the egress PE router.
- If you configure a virtual loopback tunnel interface on the egress PE router, and the egress PE router is also a transit router for the point-to-multipoint LSP, the penultimate

hop router sends just one copy of each packet over the link to the egress PE router. A virtual loopback tunnel interface can perform two lookups on an incoming packet, one for the multicast MPLS lookup and one for the IP lookup.



NOTE: Junos OS Release 11.2 and earlier do not support point-to-multipoint LSPs with next-generation multicast VPNs on MX80 routers.

The following sections describe how to configure point-to-multipoint LSPs for MBGP MVPNs:

- [Configuring RSVP-Signaled Inclusive Point-to-Multipoint LSPs for an MBGP MVPN on page 77](#)
- [Configuring Selective Provider Tunnels for an MBGP MVPN on page 78](#)

Configuring RSVP-Signaled Inclusive Point-to-Multipoint LSPs for an MBGP MVPN

You can configure LDP-signaled or RSVP-signaled inclusive point-to-multipoint LSPs for MBGP MVPNs. Aggregation is not supported, so you need to configure an inclusive point-to-multipoint LSP for each sender PE router in each multicast VPN routing instance. The sender PE router is in the sender site set of the MBGP MVPN.

To configure a static RSVP-signaled inclusive point-to-multipoint LSP, include the **static-lsp** statement:

```
static-lsp lsp-name;
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel rsvp-te]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel rsvp-te]

To configure dynamic inclusive point-to-multipoint LSPs, include the **label-switched-path-template** statement:

```
label-switched-path-template (Multicast) {  
  (default-template | lsp-template-name);  
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel rsvp-te]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel rsvp-te]

You can configure either the **default-template** option or manually configure a point-to-multipoint LSP template and specify the template name.

Configuring Selective Provider Tunnels for an MBGP MVPN

You can configure LDP-signaled or RSVP-signaled selective point-to-multipoint LSPs (also referred to as selective provider tunnels) for MBGP MVPNs. Selective point-to-multipoint LSPs send traffic only to the receivers configured for the multicast VPNs, helping to minimize flooding in the service provider's network.

As with inclusive point-to-multipoint LSPs, you can configure both dynamic and static selective tunnels for the multicast VPN.

To configure selective point-to-multipoint provider tunnels, include the **selective** statement:

```
selective {
  group multicast--prefix/prefix-length {
    source ip--prefix/prefix-length {
      ldp-p2mp;
      pim-ssm {
        group-range multicast-prefix;
      }
      rsvp-te {
        label-switched-path-template {
          (default-template | lsp-template-name);
        }
        static-lsp point-to-multipoint-lsp-name;
      }
      threshold-rate kbits;
    }
  }
  wildcard-source {
    ldp-p2mp;
    pim-ssm {
      group-range multicast-prefix;
    }
    rsvp-te {
      label-switched-path-template {
        (default-template | lsp-template-name);
      }
      static-lsp point-to-multipoint-lsp-name;
    }
    threshold-rate kbits;
  }
}
tunnel-limit number;
wildcard-group-inet {
  wildcard-source {
    ldp-p2mp;
    pim-ssm {
      group-range multicast-prefix;
    }
    rsvp-te {
      label-switched-path-template {
        (default-template | lsp-template-name);
      }
      static-lsp lsp-name;
    }
  }
}
```

```

    }
    threshold-rate number;
  }
}
wildcard-group-inet6 {
  wildcard-source {
    ldp-p2mp;
    pim-ssm {
      group-range multicast-prefix;
    }
    rsvp-te {
      label-switched-path-template {
        (default-template | lsp-template-name);
      }
      static-lsp lsp-name;
    }
    threshold-rate number;
  }
}
}

```

You can include these statements at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel]

The following sections describe how to configure selective point-to-multipoint LSPs for MBGP MVPNs:

- [Configuring the Multicast Group Address for an MBGP MVPN on page 79](#)
- [Configuring the Multicast Source Address for an MBGP MVPN on page 80](#)
- [Configuring Static Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 80](#)
- [Configuring Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 80](#)
- [Configuring the Threshold for Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 81](#)
- [Configuring the Tunnel Limit for Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 81](#)

Configuring the Multicast Group Address for an MBGP MVPN

To configure a point-to-multipoint LSP for an MBGP MVPN, you need to specify a multicast group address by including the **group** statement:

```
group address { ... }
```

You can include this statements at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel selective]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel selective]

The address must be a valid multicast group address. Multicast uses the Class D IP address range (224.0.0.0 through 239.255.255.255).

Configuring the Multicast Source Address for an MBGP MVPN

To configure a point-to-multipoint LSP for an MBGP MVPN, specify a multicast source address by including the **source** statement:

```
source address { ... }
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel selective group address]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel selective group address]

Configuring Static Selective Point-to-Multipoint LSPs for an MBGP MVPN

You can configure a static selective point-to-multipoint LSP for an MBGP MVPN. You need to configure a static LSP using the standard MPLS LSP statements at the [edit protocols mpls] hierarchy level. You then include the static LSP in your selective point-to-multipoint LSP configuration by using the **static-lsp** statement. Once this functionality is enabled on the source PE router, the static point-to-multipoint LSP is created based on your configuration.

To configure a static selective point-to-multipoint LSP, include the **rsvp-te** and the **static-lsp** statements:

```
rsvp-te static-lsp lsp-name;
```

You can include these statements at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel selective group address source *source-address*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel selective group address source *source-address*]

Configuring Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN

You can configure a dynamic selective point-to-multipoint LSP for an MBGP MVPN. The leaf nodes for a dynamic point-to-multipoint LSP can be automatically discovered using leaf automatic discovery routes. Selective provider multicast service interface (S-PMSI) automatic discovery routes are also supported.

To configure a dynamic selective point-to-multipoint provider tunnel, include the **rsvp-te** and **label-switched-path-template** statements:

```
rsvp-te label-switched-path-template {  
  (default-template | lsp-template-name);  
}
```


You can include these statements at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel selective group address source *source-address*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel selective group address source *source-address*]

The **label-switched-path-template** statement includes the following options:

- **default-template**—Specify that point-to-multipoint LSPs are generated dynamically based on the default template. No user configuration is required for the LSPs. However, the automatically generated LSPs include none of the common LSP features, such as bandwidth allocation and traffic engineering.
- **lsp-template-name**—Specify the name of an LSP template to be used for the point-to-multipoint LSP. You need to configure the LSP template to be used as a basis for the point-to-multipoint LSPs. You can configure any of the common LSP features for this template.

Configuring the Threshold for Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN

To configure a selective point-to-multipoint LSP dynamically, you need to specify the data threshold (in kilobits per second) required before a new tunnel is created using the **threshold-rate** statement:

threshold-rate *number*;

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel selective group address source *source-address*]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel selective group address source *source-address*]

Configuring the Tunnel Limit for Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN

To configure a limit on the number of tunnels that can be generated for a dynamic point-to-multipoint LSP, include the **tunnel-limit** statement:

tunnel-limit *number*;

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel selective]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel selective]

Related Documentation

- *Example: Configuring Point-to-Multipoint LDP LSPs as the Data Plane for Intra-AS MBGP MVPNs*

Configuring PIM Provider Tunnels for an MBGP MVPN

To configure a Protocol Independent Multicast (PIM) sparse mode provider tunnel for a multicast VPN, include the **pim-asm** statement:

```
pim-asm {  
    group-address address;  
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-instances *routing-instance-name* provider-tunnel]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* provider-tunnel]

To complete the PIM sparse mode provider tunnel configuration, you also need to specify the group address using the **group-address** option. The source address for a PIM sparse mode provider tunnel is configured to be the loopback address of the loopback interface in the inet.0 routing table.

Configuring PIM-SSM GRE Selective Provider Tunnels

This topic describes how to configure a PIM-SSM GRE selective provider tunnel for an MBGP MVPN.

Creating a selective provider tunnel enables you to move high-rate traffic off the inclusive tunnel and deliver the multicast traffic only to receivers that request it. This improves bandwidth utilization.

To configure a PIM-SSM GRE selective provider tunnel for the 224.1.1.1/32 customer multicast group address, the 10.2.2.2/32 customer source address, and a virtual routing instance named **green**:

1. Configure the multicast group address range to be used for creating selective tunnels. The address prefix can be any valid nonreserved IPv4 multicast address range. Whether you configure a range of addresses or a single address, make sure that you configure enough group addresses for all the selective tunnels needed.

```
user@host# set routing-instances green provider-tunnel selective group 224.1.1.1/32  
source 10.2.2.2/32 pim-ssm group-range 232.1.1.0/24
```

2. Configure the threshold rate in kilobits per second (Kbps) for triggering the creation of the selective tunnel. If you set the threshold rate to zero Kbps, the selective tunnel is created immediately, and the multicast traffic does not use an inclusive tunnel at all. Optionally, you can leave the threshold rate unconfigured and the result is the same as setting the threshold to zero.

```
user@host# set routing-instances green provider-tunnel selective group 224.1.1.1/32  
source 10.2.2.2/32 threshold-rate 0
```

3. Configure the autonomous system number in the global routing options. This is required in MBGP MVPNs.

```
user@host# set routing-options autonomous-system 100
```

When configuring PIM-SSM GRE selective provider tunnels, keep the following in mind:

- Aggregation of multiple customer multicast routes to a single PIM S-PMSI is not supported.
- Provider tunnel multicast group addresses must be IPv4 addresses, even in configurations in which the customer multicast group and source are IPv6 addresses.

**Related
Documentation**

- [Multicast VPN Terminology on page 4](#)
- [pim-ssm on page 133](#)
- [group-range on page 120](#)
- [threshold-rate on page 148](#)

CHAPTER 7

Configuring Draft Rosen VPNs

- [Example: Configuring PIM Join Load Balancing on Draft-Rosen Multicast VPN on page 85](#)

Example: Configuring PIM Join Load Balancing on Draft-Rosen Multicast VPN

This example shows how to configure multipath routing for external and internal virtual private network (VPN) routes with unequal interior gateway protocol (IGP) metrics, and Protocol Independent Multicast (PIM) join load balancing on provider edge (PE) routers running Draft-Rosen multicast VPN (MVPN). This feature allows customer PIM (C-PIM) join messages to be load-balanced across external and internal BGP (EIBGP) upstream paths when the PE router has both external BGP (EBGP) and internal BGP (IBGP) paths toward the source or rendezvous point (RP).

- [Requirements on page 85](#)
- [Overview and Topology on page 86](#)
- [Configuration on page 89](#)
- [Verification on page 92](#)

Requirements

This example requires the following hardware and software components:

- Three routers that can be a combination of M Series Multiservice Edge Routers, MX Series 3D Universal Edge Routers, or T Series Core Routers.
- Junos OS Release 12.1 or later running on all the devices.

Before you begin:

1. Configure the device interfaces.
2. Configure the following routing protocols on all PE routers:
 - OSPF
 - MPLS
 - LDP
 - PIM
 - BGP

3. Configure a multicast VPN.

Overview and Topology

Junos OS Release 12.1 and later support multipath configuration along with PIM join load balancing. This allows C-PIM join messages to be load-balanced across unequal EIBGP routes, if a PE router has EBGP and IBGP paths toward the source (or RP). In previous releases, only the active EBGP path was used to send the join messages. This feature is applicable to IPv4 C-PIM join messages.

During load balancing, if a PE router loses one or more EBGP paths toward the source (or RP), the C-PIM join messages that were previously using the EBGP path are moved to a multicast tunnel interface, and the reverse path forwarding (RPF) neighbor on the multicast tunnel interface is selected based on a hash mechanism.

On discovering the first EBGP path toward the source (or RP), only the new join messages get load-balanced across EIBGP paths, whereas the existing join messages on the multicast tunnel interface remain unaffected.

Though the primary goal for multipath PIM join load balancing is to utilize unequal EIBGP paths for multicast traffic, potential join loops can be avoided if a PE router chooses only the EBGP path when there are one or more join messages for different groups from a remote PE router. If the remote PE router's join message arrives after the PE router has already chosen IBGP as the upstream path, then the potential loops can be broken by changing the selected upstream path to EBGP.



NOTE: During a graceful Routing Engine switchover (GRES), the EIBGP path selection for C-PIM join messages can vary, because the upstream interface selection is performed again for the new Routing Engine based on the join messages it receives from the CE and PE neighbors. This can lead to disruption of multicast traffic depending on the number of join messages received and the load on the network at the time of the graceful restart. However, the nonstop active routing feature is not supported and has no impact on the multicast traffic in a Draft-Rosen MVPN scenario.

In this example, PE1 and PE2 are the upstream PE routers for which the multipath PIM join load-balancing feature is configured. Routers PE1 and PE2 have one EBGP path and one IBGP path each toward the source. The Source and Receiver attached to customer edge (CE) routers are Free BSD hosts.

On PE routers that have EIBGP paths toward the source (or RP), such as PE1 and PE2, PIM join load balancing is performed as follows:

1. The existing join-count-based load balancing is performed such that the algorithm first selects the least loaded C-PIM interface. If there is equal or no load on all the C-PIM interfaces, the join messages get distributed equally across the available upstream interfaces.

In [Figure 6 on page 89](#), if the PE1 router receives PIM join messages from the CE2 router, and if there is equal or no load on both the EBG and IBGP paths toward the source, the join messages get load-balanced on the EIBGP paths.

2. If the selected least loaded interface is a multicast tunnel interface, then there can be a potential join loop if the downstream list of the customer join (C-join) message already contains the multicast tunnel interface. In such a case, the least loaded interface among EBG paths is selected as the upstream interface for the C-join message.

Assuming that the IBGP path is the least loaded, the PE1 router sends the join messages to PE2 using the IBGP path. If PIM join messages from the PE3 router arrive on PE1, then the downstream list of the C-join messages for PE3 already contains a multicast tunnel interface, which can lead to a potential join loop, because both the upstream and downstream interfaces are multicast tunnel interfaces. In this case, PE1 uses only the EBG path to send the join messages.

3. If the selected least loaded interface is a multicast tunnel interface and the multicast tunnel interface is not present in the downstream list of the C-join messages, the loop prevention mechanism is not necessary. If any PE router has already advertised data multicast distribution tree (MDT) type, length, and values (TLVs), that PE router is selected as the upstream neighbor.

When the PE1 router sends the join messages to PE2 using the least loaded IBGP path, and if PE3 sends its join messages to PE2, no join loop is created.

4. If no data MDT TLV corresponds to the C-join message, the least loaded neighbor on a multicast tunnel interface is selected as the upstream interface.

On PE routers that have only IBGP paths toward the source (or RP), such as PE3, PIM join load balancing is performed as follows:

1. The PE router only finds a multicast tunnel interface as the RPF interface, and load balancing is done across the C-PIM neighbors on a multicast tunnel interface.

Router PE3 load-balances PIM join messages received from the CE4 router across the IBGP paths to the PE1 and PE2 routers.

2. If any PE router has already advertised data MDT TLVs corresponding to the C-join messages, that PE router is selected as the RPF neighbor.

For a particular C-multicast flow, at least one of the PE routers having EIBGP paths toward the source (or RP) must use only the EBG path to avoid or break join loops. As a result of the loop avoidance mechanism, a PE router is constrained to choose among EIBGP paths when a multicast tunnel interface is already present in the downstream list.

In [Figure 6 on page 89](#), assuming that the CE2 host is interested in receiving traffic from the Source and CE2 initiates multiple PIM join messages for different groups (Group 1 with group address 225.1.1.1, and Group 2 with group address 225.1.1.2), the join messages for both groups arrive on the PE1 router.

Router PE1 then equally distributes the join messages between the EIBGP paths toward the Source. Assuming that Group 1 join messages are sent to the CE1 router directly using the EBGp path, and Group 2 join messages are sent to the PE2 router using the IBGP path, PE1 and PE2 become the RPF neighbors for Group 1 and Group 2 join messages, respectively.

When the CE3 router initiates Group 1 and Group 2 PIM join messages, the join messages for both groups arrive on the PE2 router. Router PE2 then equally distributes the join messages between the EIBGP paths toward the Source. Since PE2 is the RPF neighbor for Group 2 join messages, it sends the Group 2 join messages directly to the CE1 router using the EBGp path. Group 1 join messages are sent to the PE1 router using the IBGP path.

However, if the CE4 router initiates multiple Group 1 and Group 2 PIM join messages, there is no control over how these join messages received on the PE3 router get distributed to reach the Source. The selection of the RPF neighbor by PE3 can affect PIM join load balancing on EIBGP paths.

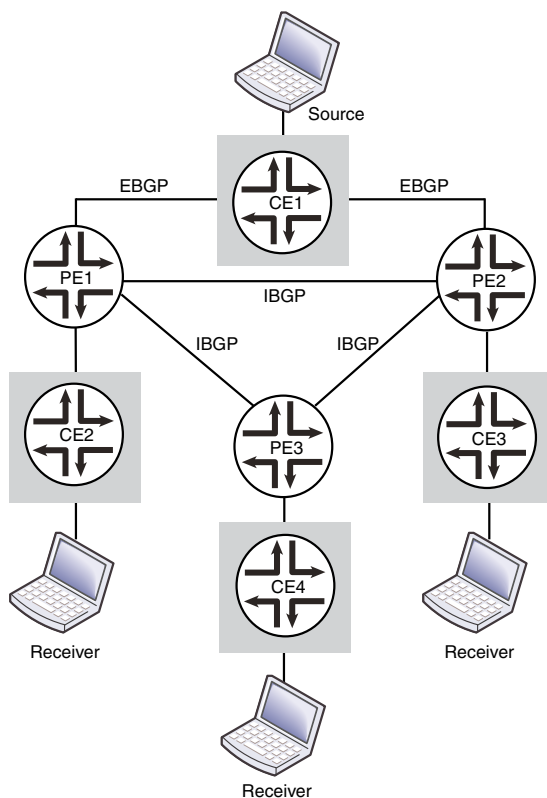
- If PE3 sends Group 1 join messages to PE1 and Group 2 join messages to PE2, there is no change in RPF neighbor. As a result, no join loops are created.
- If PE3 sends Group 1 join messages to PE2 and Group 2 join messages to PE1, there is a change in the RPF neighbor for the different groups resulting in the creation of join loops. To avoid potential join loops, PE1 and PE2 do not consider IBGP paths to send the join messages received from the PE3 router. Instead, the join messages are sent directly to the CE1 router using only the EBGp path.

The loop avoidance mechanism in a Draft-Rosen MVPN has the following limitations:

- Because the timing of arrival of join messages on remote PE routers determines the distribution of join messages, the distribution could be sub-optimal in terms of join count.
- Because join loops cannot be avoided and can occur due to the timing of join messages, the subsequent RPF interface change leads to loss of multicast traffic. This can be avoided by implementing the PIM make-before-break feature.

The PIM make-before-break feature is an approach to detect and break C-PIM join loops in a Draft-Rosen MVPN. The C-PIM join messages are sent to the new RPF neighbor after establishing the PIM neighbor relationship, but before updating the related multicast forwarding entry. Though the upstream RPF neighbor would have updated its multicast forwarding entry and started sending the multicast traffic downstream, the downstream router does not forward the multicast traffic (because of RPF check failure) until the multicast forwarding entry is updated with the new RPF neighbor. This helps to ensure that the multicast traffic is available on the new path before switching the RPF interface of the multicast forwarding entry.

Figure 6: PIM Join Load Balancing on Draft-Rosen MVPN



9040919

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```

PE1 set routing-instances vpn1 instance-type vrf
    set routing-instances vpn1 interface ge-5/0/4.0
    set routing-instances vpn1 interface ge-5/2/0.0
    set routing-instances vpn1 interface lo0.1
    set routing-instances vpn1 route-distinguisher 1:1
    set routing-instances vpn1 vrf-target target:1:1
    set routing-instances vpn1 routing-options multipath vpn-unequal-cost
        equal-external-internal
    set routing-instances vpn1 protocols bgp export direct
    set routing-instances vpn1 protocols bgp group bgp type external
    set routing-instances vpn1 protocols bgp group bgp local-address 44.44.44.1
    set routing-instances vpn1 protocols bgp group bgp family inet unicast
    set routing-instances vpn1 protocols bgp group bgp neighbor 44.44.44.2 peer-as 3
    set routing-instances vpn1 protocols bgp group bgp1 type external
    set routing-instances vpn1 protocols bgp group bgp1 local-address 11.11.11.1
    set routing-instances vpn1 protocols bgp group bgp1 family inet unicast
    set routing-instances vpn1 protocols bgp group bgp1 neighbor 11.11.11.2 peer-as 4
    set routing-instances vpn1 protocols pim vpn-group-address 224.1.1.1
    set routing-instances vpn1 protocols pim rp static address 10.255.8.168
  
```

```
set routing-instances vpn1 protocols pim interface all
set routing-instances vpn1 protocols pim join-load-balance
```

```
PE2 set routing-instances vpn1 instance-type vrf
set routing-instances vpn1 interface ge-2/0/3.0
set routing-instances vpn1 interface ge-4/0/5.0
set routing-instances vpn1 interface lo0.1
set routing-instances vpn1 route-distinguisher 2:2
set routing-instances vpn1 vrf-target target:1:1
set routing-instances vpn1 routing-options multipath vpn-unequal-cost
    equal-external-internal
set routing-instances vpn1 protocols bgp export direct
set routing-instances vpn1 protocols bgp group bgp1 type external
set routing-instances vpn1 protocols bgp group bgp1 local-address 10.90.10.1
set routing-instances vpn1 protocols bgp group bgp1 family inet unicast
set routing-instances vpn1 protocols bgp group bgp1 neighbor 10.90.10.2 peer-as 45
set routing-instances vpn1 protocols bgp group bgp type external
set routing-instances vpn1 protocols bgp group bgp local-address 10.50.10.2
set routing-instances vpn1 protocols bgp group bgp family inet unicast
set routing-instances vpn1 protocols bgp group bgp neighbor 10.50.10.1 peer-as 4
set routing-instances vpn1 protocols pim vpn-group-address 224.1.1.1
set routing-instances vpn1 protocols pim rp static address 10.255.8.168
set routing-instances vpn1 protocols pim interface all
set routing-instances vpn1 protocols pim join-load-balance
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*. To configure the PE1 router:



NOTE: Repeat this procedure for every Juniper Networks router in the MVPN domain, after modifying the appropriate interface names, addresses, and any other parameters for each router.

1. Configure a VPN routing and forwarding (VRF) instance.


```
[edit routing-instances vpn1]
user@PE1# set instance-type vrf
user@PE1# set interface ge-5/0/4.0
user@PE1# set interface ge-5/2/0.0
user@PE1# set interface lo0.1
user@PE1# set route-distinguisher 1:1
user@PE1# set vrf-target target:1:1
```
2. Enable protocol-independent load balancing for the VRF instance.


```
[edit routing-instances vpn1]
user@PE1# set routing-options multipath vpn-unequal-cost equal-external-internal
```
3. Configure BGP groups and neighbors to enable PE to CE routing.


```
[edit routing-instances vpn1 protocols]
user@PE1# set bgp export direct
user@PE1# set bgp group bgp type external
user@PE1# set bgp group bgp local-address 44.44.44.1
```

```

user@PE1# set bgp group bgp family inet unicast
user@PE1# set bgp group bgp neighbor 44.44.44.2 peer-as 3
user@PE1# set bgp group bgp1 type external
user@PE1# set bgp group bgp1 local-address 11.11.11.1
user@PE1# set bgp group bgp1 family inet unicast
user@PE1# set bgp group bgp1 neighbor 11.11.11.2 peer-as 4

```

4. Configure PIM to enable PE to CE multicast routing.

```

[edit routing-instances vpn1 protocols]
user@PE1# set pim vpn-group-address 224.1.1.1
user@PE1# set pim rp static address 10.255.8.168

```

5. Enable PIM on all network interfaces.

```

[edit routing-instances vpn1 protocols]
user@PE1# set pim interface all

```

6. Enable PIM join load balancing for the VRF instance.

```

[edit routing-instances vpn1 protocols]
user@PE1# set pim join-load-balance

```

Results From configuration mode, confirm your configuration by entering the **show routing-instances** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```

routing-instances {
  vpn1 {
    instance-type vrf;
    interface ge-5/0/4.0;
    interface ge-5/2/0.0;
    interface lo0.1;
    route-distinguisher 1:1;
    vrf-target target:1:1;
    routing-options {
      multipath {
        vpn-unequal-cost equal-external-internal;
      }
    }
  }
  protocols {
    bgp {
      export direct;
      group bgp {
        type external;
        local-address 44.44.44.1;
        family inet {
          unicast;
        }
        neighbor 44.44.44.2 {
          peer-as 3;
        }
      }
    }
    group bgp1 {
      type external;
      local-address 11.11.11.1;
      family inet {

```

```

        unicast;
    }
    neighbor 11.11.11.2 {
        peer-as 4;
    }
}
}
pim {
    vpn-group-address 224.1.1.1;
    rp {
        static {
            address 10.255.8.168;
        }
    }
    interface all;
    join-load-balance;
}
}
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

Confirm that the configuration is working properly.

- [Verifying PIM Join Load Balancing for Different Groups of Join Messages on page 92](#)

Verifying PIM Join Load Balancing for Different Groups of Join Messages

Purpose Verify PIM join load balancing for the different groups of join messages received on the PE1 router.

Action From operational mode, run the **show pim join instance extensive** command.

```

user@PE1> show pim join instance extensive
Instance: PIM.vpn1 Family: INET
R = Rendezvous Point Tree, S = Sparse, W = Wildcard

Group: 225.1.1.1
Source: *
RP: 10.255.8.168
Flags: sparse,rptree,wildcard
Upstream interface: ge-5/2/0.1
Upstream neighbor: 10.10.10.2
Upstream state: Join to RP
Downstream neighbors:
Interface: ge-5/0/4.0
10.40.10.2 State: Join Flags: SRW Timeout: 207

Group: 225.1.1.2
Source: *
RP: 10.255.8.168
Flags: sparse,rptree,wildcard
Upstream interface: mt-5/0/10.32768
Upstream neighbor: 19.19.19.19

```

```

Upstream state: Join to RP
Downstream neighbors:
  Interface: ge-5/0/4.0
    10.40.10.2 State: Join Flags: SRW Timeout: 207

Group: 225.1.1.3
Source: *
RP: 10.255.8.168
Flags: sparse,rptree,wildcard
Upstream interface: ge-5/2/0.1
Upstream neighbor: 10.10.10.2
Upstream state: Join to RP
Downstream neighbors:
  Interface: ge-5/0/4.0
    10.40.10.2 State: Join Flags: SRW Timeout: 207

Group: 225.1.1.4
Source: *
RP: 10.255.8.168
Flags: sparse,rptree,wildcard
Upstream interface: mt-5/0/10.32768
Upstream neighbor: 19.19.19.19
Upstream state: Join to RP
Downstream neighbors:
  Interface: ge-5/0/4.0
    10.40.10.2 State: Join Flags: SRW Timeout: 207

```

Meaning The output shows how the PE1 router has load-balanced the C-PIM join messages for four different groups.

- For Group 1 (group address: 225.1.1.1) and Group 3 (group address: 225.1.1.3) join messages, the PE1 router has selected the EBGp path toward the CE1 router to send the join messages.
- For Group 2 (group address: 225.1.1.2) and Group 4 (group address: 225.1.1.4) join messages, the PE1 router has selected the IBGP path toward the PE2 router to send the join messages.

Related Documentation

- *PIM Join Load Balancing on Multipath MVPN Routes Overview*
- [Example: Configuring PIM Join Load Balancing On Next-Generation Multicast VPN on page 20](#)

Configuring GRE Tunnel Interfaces for Layer 3 VPNs

- [Configuring GRE Tunnels for Layer 3 VPNs on page 95](#)

Configuring GRE Tunnels for Layer 3 VPNs

Junos OS allows you to configure a generic routing encapsulation (GRE) tunnel between the PE and CE routers for a Layer 3 VPN. The GRE tunnel can have one or more hops. You can configure the tunnel from the PE router to a local CE router (as shown in [Figure 7 on page 95](#)) or to a remote CE router (as shown in [Figure 8 on page 95](#)).

Figure 7: GRE Tunnel Configured Between the Local CE Router and the PE Router

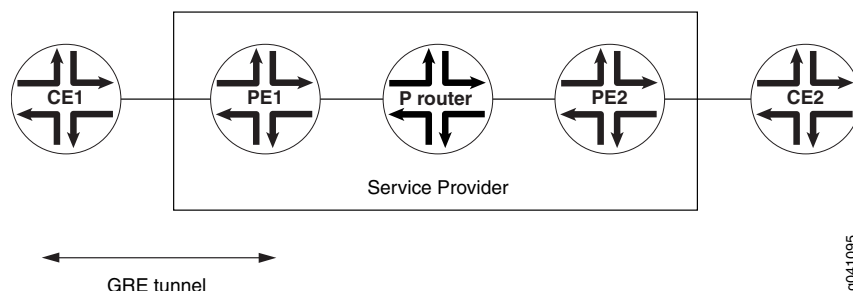
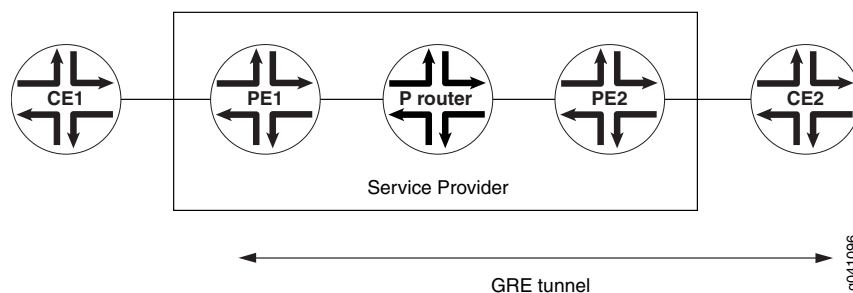


Figure 8: GRE Tunnel Configured Between the Remote CE Router and the PE Router



For more information about how to configure tunnel interfaces, see the *Junos OS Services Interfaces Library for Routing Devices*.

You can configure the GRE tunnels manually or configure the Junos OS to instantiate GRE tunnels dynamically.

The following sections describe how to configure GRE tunnels manually and dynamically:

- [Configuring GRE Tunnels Manually Between PE and CE Routers on page 96](#)
- [Configuring GRE Tunnels Dynamically on page 97](#)

Configuring GRE Tunnels Manually Between PE and CE Routers

You can manually configure a GRE tunnel between a PE router and either a local CE router or a remote CE router for a Layer 3 VPN as explained in the following sections:

- [Configuring the GRE Tunnel Interface on the PE Router on page 96](#)
- [Configuring the GRE Tunnel Interface on the CE Router on page 97](#)

Configuring the GRE Tunnel Interface on the PE Router

You configure the GRE tunnel as a logical interface on the PE router. To configure the GRE tunnel interface, include the **unit** statement:

```
unit logical-unit-number {  
  tunnel {  
    source source-address;  
    destination destination-address;  
    routing-instance {  
      destination routing-instance-name;  
    }  
  }  
  family inet {  
    address address;  
  }  
}
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name*]**

As part of the GRE tunnel interface configuration, you need to include the following statements:

- **source *source-address***—Specify the source or origin of the GRE tunnel, typically the PE router.
- **destination *destination-address***—Specify the destination or end point of the GRE tunnel. The destination can be a Provider router, the local CE router, or the remote CE router.

By default, the tunnel destination address is assumed to be in the default Internet routing table, `inet.0`. If the tunnel destination address is not in `inet.0`, you need to specify which routing table to search for the tunnel destination address by configuring the **routing-instance** statement. This is the case if the tunnel encapsulating interface is also configured under the routing instance.

- **destination *routing-instance-name***—Specify the name of the routing instance when configuring the GRE tunnel interface on the PE router.

To complete the GRE tunnel interface configuration, include the **interface** statement for the GRE interface under the appropriate routing instance:

```
interface interface-name;
```

You can include this statement at the following hierarchy levels:

- **[edit routing-instances *routing-instance-name*]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*]**

Configuring the GRE Tunnel Interface on the CE Router

You can configure either the local or the remote CE router to act as the endpoint for the GRE tunnel.

To configure the GRE tunnel interface on the CE router, include the **unit** statement:

```
unit logical-unit-number {
  tunnel {
    source address;
    destination address;
  }
  family inet {
    address address;
  }
}
```

You can include this statement at the following hierarchy levels:

- **[edit interfaces *interface-name*]**
- **[edit logical-systems *logical-system-name* interfaces *interface-name*]**

Configuring GRE Tunnels Dynamically

When the router receives a VPN route to a BGP next hop address, but no MPLS path is available, a GRE tunnel can be dynamically generated to carry the VPN traffic across the BGP network. The GRE tunnel is generated and then its routing information is copied into the `inet.3` routing table. IPv4 routes are the only type of routes supported for dynamic GRE tunnels. Also, the routing platform must have a tunnel PIC.



NOTE: When configuring a dynamic GRE tunnel to a remote CE router, do not configure OSPF over the tunnel interface. It creates a routing loop forcing the router to take the GRE tunnel down. The router attempts to reestablish the GRE tunnel, but will be forced to take it down again when OSPF becomes active on the tunnel interface and discovers a route to the tunnel endpoint. This is not an issue when configuring static GRE tunnels to a remote CE router.

To generate GRE tunnels dynamically, include the **dynamic-tunnels** statement:

```
dynamic-tunnels tunnel-name {  
    destination-networks prefix;  
    source-address address;  
}
```

You can include this statement at the following hierarchy levels:

- [edit routing-options]
- [edit logical-systems *logical-system-name* routing-options]

Specify the IPv4 prefix range (for example, 10/8 or 11.1/16) for the destination network by including the **destination-networks** statement. Only tunnels within the specified IPv4 prefix range are allowed to be initiated.

```
destination-networks prefix;
```

You can include this statement at the following hierarchy levels:

- [edit routing-options dynamic-tunnels *tunnel-name*]
- [edit logical-systems *logical-system-name* routing-options dynamic-tunnels *tunnel-name*]

Specify the source address for the GRE tunnels by including the **source-address** statement. The source address specifies the address used as the source for the local tunnel endpoint. This could be any local address on the router (typically the router ID or the loopback address).

```
source-address address;
```

You can include this statement at the following hierarchy levels:

- [edit routing-options dynamic-tunnels *tunnel-name*]
- [edit logical-systems *logical-system-name* routing-options dynamic-tunnels *tunnel-name*]

Related Documentation

- *Example: Configuring a Two-Tiered Virtualized Data Center for Large Enterprise Networks*

PART 3

Troubleshooting

- [Tracing Operations on page 101](#)

Tracing Operations

- [Tracing MBGP MVPN Traffic and Operations on page 101](#)

Tracing MBGP MVPN Traffic and Operations

To trace MBGP MVPN traffic, you can specify options with the **traceoptions** statement:

1. Specify the name of one or more MVPN trace files using the **file** option for the **traceoptions** at the **[edit routing-instances *routing-instance-name* protocols mvpn]** hierarchy level or at the **[edit protocols mvpn]** hierarchy level:

```
traceoptions {
  file filename <files number> <size size> <world-readable | no-world-readable>;
}
```

The **file** option includes the following sub-options:

- ***filename***—Specify the name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory **/var/log**.
 - ***files number***—(Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum ***size***, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the specified maximum ***number*** of trace files specified is reached. Then the oldest trace file is overwritten.
 - ***size size***—(Optional) Maximum size of each trace file. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.
 - ***world-readable | no-world-readable***—(Optional) Enable unrestricted file access or restrict file access to the user who created the file.
2. Specify the **flag** option for the **traceoptions** statement:

```
traceoptions {
  flag flag <flag-modifier> <disable>;
}
```

The following trace flags display the operations associated with multicast VPNs:

- **all**—All multicast VPN tracing options
- **cmcast-join**—Multicast VPN C-multicast join routes

- **error**—Error conditions
- **general**—General events
- **inter-as-ad**—Multicast VPN inter-AS automatic discovery routes
- **intra-as-ad**—Multicast VPN intra-AS automatic discovery routes
- **leaf-ad**—Multicast VPN leaf automatic discovery routes
- **mdt-safi-ad**—Multicast VPN MDT SAFI automatic discovery routes
- **nlri**—Multicast VPN advertisements received or sent by means of BGP
- **normal**—Normal events
- **policy**—Policy processing
- **route**—Routing information
- **source-active**—Multicast VPN source active routes
- **spmsi-ad**—Multicast VPN SPMSI auto discovery active routes
- **state**—State transitions
- **task**—Routing protocol task processing
- **timer**—Routing protocol timer processing
- **tunnel**—Provider tunnel events
- **umh**—Upstream multicast hop (UMH) events

Related Documentation • [traceoptions on page 149](#)

PART 4

Configuration Statements and Operational Commands

- Configuration Statements on page 105
- Operational Commands on page 157

CHAPTER 10

Configuration Statements

- [\[edit protocols bgp\] Hierarchy Level on page 106](#)
- [Layer 2 Routing Instances Configuration Hierarchy on page 113](#)
- [advertise-from-main-vpn-tables on page 116](#)
- [create-new-ucast-tunnel on page 117](#)
- [export-target on page 118](#)
- [family \(VRF Advertisement\) on page 118](#)
- [group \(Routing Instances\) on page 119](#)
- [group-range \(MBGP MVPN Tunnel\) on page 120](#)
- [group-rp-mapping on page 121](#)
- [import-target on page 122](#)
- [inet-mvpn \(BGP\) on page 123](#)
- [inet-mvpn \(VRF Advertisement\) on page 124](#)
- [inet6-mvpn \(BGP\) on page 124](#)
- [inet6-mvpn \(VRF Advertisement\) on page 125](#)
- [ingress-replication on page 126](#)
- [interface \(Virtual Tunnel in Routing Instances\) on page 127](#)
- [label-switched-path-template \(Multicast\) on page 128](#)
- [mpls-internet-multicast on page 129](#)
- [multicast \(Virtual Tunnel in Routing Instances\) on page 129](#)
- [mvpn \(NG-MVPN\) on page 130](#)
- [mvpn-mode on page 132](#)
- [pim-asm on page 132](#)
- [pim-ssm \(Selective Tunnel\) on page 133](#)
- [primary \(Virtual Tunnel in Routing Instances\) on page 134](#)
- [provider-tunnel on page 135](#)
- [register-limit on page 138](#)
- [route-target \(Protocols MVPN\) on page 139](#)
- [rpt-spt on page 140](#)

- [rsvp-te \(Routing Instances Provider Tunnel Selective\)](#) on page 141
- [selective](#) on page 142
- [sglimit](#) on page 144
- [source \(Routing Instances Provider Tunnel Selective\)](#) on page 145
- [spt-only](#) on page 146
- [static-lsp](#) on page 146
- [target \(Routing Instances MVPN\)](#) on page 147
- [threshold-rate](#) on page 148
- [traceoptions \(Protocols MVPN\)](#) on page 149
- [tunnel-limit \(Routing Instances Provider Tunnel Selective\)](#) on page 151
- [unicast \(Route Target Community\)](#) on page 152
- [unicast \(Virtual Tunnel in Routing Instances\)](#) on page 152
- [vrf-advertise-selective](#) on page 153
- [wildcard-group-inet](#) on page 154
- [wildcard-group-inet6](#) on page 155
- [wildcard-source \(Selective Provider Tunnels\)](#) on page 156

[\[edit protocols bgp\] Hierarchy Level](#)

Several statements in the [\[edit protocols mpls\]](#) hierarchy are valid at numerous locations within it. To make the complete hierarchy easier to read, the repeated statements are listed in “[Common BGP Family Options](#)” on page 106 and that section is referenced at the appropriate locations in “[Complete \[edit protocols bgp\] Hierarchy](#)” on page 107.

- [Common BGP Family Options](#) on page 106
- [Complete \[edit protocols bgp\] Hierarchy](#) on page 107

Common BGP Family Options

This section lists statements that are valid at the following hierarchy levels, and is referenced at those levels in “[Complete \[edit protocols bgp\] Hierarchy](#)” on page 107 instead of the statements being repeated.

- [\[edit protocols bgp family inet \(any | flow | labeled-unicast | multicast | unicast\)\]](#)
- [\[edit protocols bgp family inet6 \(any | labeled-unicast | multicast | unicast\)\]](#)
- [\[edit protocols bgp family \(evpn | inet-mdt | inet-mvpn | inet6-mvpn | l2vpn\) signaling\]](#)
- [\[edit protocols bgp family inet-vpn \(any | flow | multicast | unicast\)\]](#)
- [\[edit protocols bgp family inet6-vpn \(any | multicast | unicast\)\]](#)
- [\[edit protocols bgp family iso-vpn unicast\]](#)

The common BGP family options are as follows:

accepted-prefix-limit {

```

    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>;
}
damping;
loops number;
prefix-limit {
    maximum number;
    teardown <percentage> <idle-timeout (forever | minutes)>;
}
rib-group group-name;
topology name {
    community {
        target identifier;
    }
}
}

```

Complete [edit protocols bgp] Hierarchy

The statement hierarchy listed in this section can also be included at the **[edit logical-systems *logical-system-name*]** hierarchy level.

```

protocols {
    bgp {
        disable;
        accept-remote-nexthop;
        advertise-external <conditional>;
        advertise-from-main-vpn-tables;
        advertise-inactive;
        (advertise-peer-as | no-advertise-peer-as);
        authentication-algorithm (aes-128-cmac-96 | hmac-sha-1-96 | md5);
        authentication-key key;
        authentication-key-chain key-chain;
        bfd-liveness-detection {
            authentication {
                algorithm (keyed-md5 | keyed-sha-1 | meticulous-keyed-md5 |
                    meticulous-keyed-sha-1 | simple-password);
                key-chain key-chain-name;
                loose-check;
            }
            detection-time {
                threshold milliseconds;
            }
            holddown-interval milliseconds;
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            session-mode (automatic | multihop | single-hop);
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            version (1 | automatic);
        }
        bmp {
            monitor (disable | enable);
        }
    }
}

```

```

route-monitoring {
    none;
    post-policy {
        exclude-non-eligible;
    }
    pre-policy {
        exclude-non-feasible;
    }
}
}
cluster cluster-identifier;
damping;
description text-description;
export [ policy-names ];
family family-name {
    ... the family subhierarchies appear after the main [edit protocols bgp] hierarchy ...
}
unconfigured-peer-graceful-restart;
graceful-restart {
    disable;
    restart-time seconds;
    stale-routes-time seconds;
}
graceful-restart {
    long-lived {
        receiver {
            enable;
            disable;
        }
        advertise-to-non-llgr-neighbor {
            omit-no-export;
        }
    }
}
graceful-restart {
    disable-notification-flag;
    disable-notification-extensions {
        omit-no-export;
    }
}
forwarding-state-bit (from-fib | set); /* Configurable to be common for all address
    families */
forwarding-state-bit (as-rr-client | from-fib); /* Configurable for each address family
    */
long-lived {
    restarter {
        disable;
        stale-time interval;
    }
}
}
group group-name {
    ... the group subhierarchy appears after the main [edit protocols bgp] hierarchy ...
}
hold-time seconds;
idle-after-switch-over (seconds | forever);
import [ policy-names ];

```

```

include-mp-next-hop;
ipsec-sa ipsec-sa;
keep (all | none);
local-address address;
local-as autonomous-system <loops number> <alias> <private>;
local-interface interface-name;
local-preference local-preference;
log-updown;
metric-out (metric | igp (delay-med-update | offset) | minimum-igp offset);
mtu-discovery;
multihop {
    no-nexthop-change;
    ttl ttl-value;
}
no-aggregator-id;
no-client-reflect;
out-delay seconds;
outbound-route-filter {
    bgp-orf-cisco-mode;
    prefix-based {
        accept {
            inet;
            inet6;
        }
    }
}
passive;
path-selection {
    always-compare-med;
    as-path-ignore;
    cisco-non-deterministic;
    external-router-id;
    med-plus-igp {
        igp-multiplier number;
        med-multiplier number;
    }
}
peer-as autonomous-system;
preference preference;
remove-private;
tcp-mss segment-size;
traceoptions {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
tcp-aggressive-transmission;
vpn-apply-export;
}

bgp {
    family inet {
        (any | multicast) {
            ... statements in Common BGP Family Options on page 106 ...
        }
    }
    flow {

```

```

... statements in Common BGP Family Options on page 106 PLUS ...
no-validate [ validation-procedure-names ];
}
labeled-unicast {
... statements in Common BGP Family Options on page 106 PLUS ...
add-path {
    receive;
    send {
        path-count number;
        prefix-policy [ policy-names ];
    }
}
aggregate-label {
    community community-name;
}
aigp [disable];
explicit-null connected-only;
per-group-label;
per-prefix-label;
protection;
resolve-vpn;
rib (inet.3 | inet6.3);
traffic-statistics {
    file filename <files number> <size maximum-file-size> <world-readable |
        no-world-readable>;
    interval seconds;
}
}
unicast {
... statements in Common BGP Family Options on page 106 PLUS ...
add-path {
    receive;
    send {
        path-count number;
        prefix-policy [ policy-names ];
    }
}
topology name {
    community target identifier;
}
}
}

bgp {
    family inet6 {
        (any | multicast) {
            ... statements in Common BGP Family Options on page 106 ...
        }
        labeled-unicast {
            ... statements in Common BGP Family Options on page 106 PLUS ...
            add-path {
                receive;
                send {
                    path-count number;
                    prefix-policy [ policy-names ];
                }
            }
        }
    }
}

```

```

    }
  }
  aggregate-label {
    community community-name;
  }
  aigp [disable];
  explicit-null;
  per-group-label;
  protection;
  traffic-statistics {
    file filename <files number> <size maximum-file-size> <world-readable |
      no-world-readable>;
    interval seconds;
  }
}
unicast {
  ... statements in Common BGP Family Options on page 106 PLUS ...
  topology name {
    community target identifier;
  }
}
}
}

bgp {
  family (evpn | inet-mdt | inet-mvpn | inet6-mvpn | l2vpn) {
    auto-discovery-only; # for l2vpn
    signaling {
      ... statements in Common BGP Family Options on page 106 ...
    }
  }
}

bgp {
  family inet-vpn {
    (any | multicast | unicast) {
      ... statements in Common BGP Family Options on page 106 PLUS ...
      aggregate-label <community community-name>;
    }
    flow {
      ... statements in Common BGP Family Options on page 106 ...
    }
  }
}

bgp {
  family inet6-vpn {
    (any | multicast | unicast) {
      ... statements in Common BGP Family Options on page 106 PLUS ...
      aggregate-label <community community-name>;
    }
  }
}

bgp {
  family iso-vpn {

```

```

    unicast {
        ... statements in Common BGP Family Options on page 106 PLUS ...
        aggregate-label <community community-name>;
    }
}

bgp {
    family route-target {
        accepted-prefix-limit {
            maximum number;
            teardown <percentage> <idle-timeout (forever | minutes)>;
        }
        advertise-default;
        external-paths number;
        prefix-limit {
            maximum number;
            teardown <percentage> <idle-timeout (forever | minutes)>;
        }
        proxy-generate <route-target-policy route-target-policy-name>;
    }
}

bgp {
    group group-name {
        ... same statements as at the [edit protocols bgp] hierarchy level PLUS ...
        allow [ all ip-prefix</prefix-length> ];
        as-override;
        multipath <multiple-as>;
        neighbor address {
            ... the neighbor subhierarchy appears after the main [edit protocols bgp group
                group-name] hierarchy ...
        }
        type (external | internal);
        ... BUT NOT ...
        disable; # NOT valid at this level
        group group-name { ... } # NOT valid at this level
        path-selection { ... } # NOT valid at this level
    }

    group group-name {
        neighbor address {
            ... same statements as at the [edit protocols bgp] hierarchy level PLUS ...
            as-override;
            multipath <multiple-as>;
            ... BUT NOT ...
            disable; # NOT valid at this level
            group group-name { ... } # NOT valid at this level
            neighbor address { ... } # NOT valid at this level
            path-selection { ... } # NOT valid at this level
        }
    }
}

```


- Related Documentation**
- *Notational Conventions Used in Junos OS Configuration Hierarchies*
 - *[edit protocols] Hierarchy Level*

Layer 2 Routing Instances Configuration Hierarchy

Use the **vpls** routing instance type for point-to-multipoint LAN implementations between a set of sites in a VPN.

To configure routing instances for Layer 2 networks, include the following statements:

```
routing-instances {
  routing-instance-name {
    access {
      address-assignment {
        ... same statements as in the address-assignment subhierarchy in [edit access]
        Hierarchy Level ...
      }
      address-protection;
      description text;
      egress-protection {
        context-identifier context-id;
      }
      forwarding-options {
        ...forwarding-options...
      }
      instance-role role;
      instance-type type;
      interface interface-name;
      l2-domain-id-for-l3 id;
      l2vpn-id community;
      layer3-domain-identifier identifier;
      multicast-snooping-options {
        ... same statements as in [edit multicast-snooping-options] Hierarchy Level EXCEPT
        FOR ...
      }
      traceoptions {...} # NOT valid at this level
    }
    no-irb-layer-2-copy;
    no-local-switching;
    no-vrf-advertise;
    no-vrf-propagate-ttl;
    pbb-options {
      default-bvlan bvlan;
      peer-instance instance;
      vlan-id vlan-id isid-list [ isid-numbers ]
    }
    protocols {
      ... the protocols subhierarchy appears after the main [edit routing-instances
      routing-instance-name] hierarchy ...
    }
    provider-tunnel {
      ... the provider-tunnel subhierarchy appears after the main [edit routing-instances
      routing-instance-name] hierarchy ...
    }
  }
}
```

```

route-distinguisher (as-number:number | ip-address:number);
routing-interface interface;
routing-options {
  ... the routing-options subhierarchy appears after the main [edit routing-instances
    routing-instance-name] hierarchy ...
}
service-groups {
  service-group-name {
    pbb-service-options {
      default-isid isid-number;
      isid isid-number vlan-id-list [ vlan-ids ];
      mac-address mac-address;
    }
    service-type type;
  }
}
switch-options {
  ... same statements as in [edit switch-options] Hierarchy Level ...
}
vlan-id (id | all | none);
vlan-model one-to-one;
vlan-tags outer <tpid.>vlan-id inner <tpid.>vlan-id;
[edit vlans] Hierarchy Level {
  ... same statements as in [edit vlans] Hierarchy Level ...
}
vrf-advertise-selective {
  family {
    inet-mvpn;
    inet6-mvpn;
  }
}
vrf-export [ policy-names ];
vrf-import [ policy-names ];
vrf-propagate-ttl;
vrf-table-label;
vrf-target {
  export community-name;
  import community-name;
}
protocols {
  ... protocols-configuration ...
}
routing-options {
  ... routing-options-configuration ...
}
bridge-domains {
  bridge-domain-name {
    domain-type bridge;
    interface interface-name;
    routing-interface routing-interface-name;
    vlan-id (Bridge Domain or VLAN) (none | all | number);
    vlan-tags outer number inner number;
    bridge-options {
      interface-mac-limit limit {
        packet-action drop;
      }
    }
  }
}

```

```

interface interface-name {
  interface-mac-limit limit {
    packet-action drop;
  }
}
mac-statistics;
mac-table-size limit {
  packet-action drop;
}
no-mac-learning;
static-mac mac-address;
}
}
}
}
}

```

With the exception of the **instance-type virtual-switch** statement (which configures a virtual-switch routing instance), you can include the statements at the following hierarchy levels:


- **[edit]**
- **[edit logical-systems *logical-system-name*]**

The **instance-type virtual-switch** statement is not supported at the **[edit logical-systems *logical-system-name*]** hierarchy level.

Related Documentation

- *Routing Instances Overview*
- *Layer 2 Routing Instance Types*
- *Configuring a Layer 2 Virtual Switch*
- *Configuring a Layer 2 Control Protocol Routing Instance*

advertise-from-main-vpn-tables

Syntax	advertise-from-main-vpn-tables;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols bgp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols bgp], [edit protocols bgp], [edit routing-instances <i>routing-instance-name</i> protocols bgp],
Release Information	Statement introduced in Junos OS Release 12.3.
Description	<p>Advertise VPN routes from the main VPN tables in the master routing instance (for example, <i>bgp.l3vpn.0</i>, <i>bgp.mvpn.0</i>) instead of advertising VPN routes from the tables in the VPN routing instances (for example, <i>instance-name.inet.0</i>, <i>instance-name.mvpn.0</i>). Enable nonstop active routing (NSR) support for BGP multicast VPN (MVPN).</p> <p>When this statement is enabled, before advertising a route for a VPN prefix, the path selection algorithm is run on all routes (local and received) that have the same route distinguisher (RD).</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p> NOTE: Adding or removing this statement causes all BGP sessions that have VPN address families to be removed and then added again. On the other hand, having this statement in the configuration prevents BGP sessions from going down when route reflector (RR) or autonomous system border router (ASBR) functionality is enabled or disabled on a routing device that has VPN address families configured.</p> </div>
Default	If you do not include this statement, VPN routes are advertised from the tables in the VPN routing instances.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Understanding Junos OS Routing Tables</i> • <i>Types of VPNs</i>

create-new-ucast-tunnel

Syntax	create-new-ucast-tunnel;
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> provider-tunnel ingress-replication], [edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i> ingress-replication]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	One of two modes for building unicast tunnels when ingress replication is configured for the provider tunnel. When this statement is configured, each time a new destination is added to the multicast distribution tree, a new unicast tunnel to the destination is created in the ingress replication tunnel. The new tunnel is deleted if the destination is no longer needed. Use this mode for RSVP LSPs using ingress replication.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Ingress Replication for IP Multicast Using MBGP MVPNs</i> • Configuring Routing Instances for an MBGP MVPN on page 75 • mpls-internet-multicast on page 129 • ingress-replication on page 126

export-target

Syntax	<code>export-target { target <i>target-community</i>; unicast; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mvpn route-target], [edit routing-instances <i>routing-instance-name</i> protocols mvpn route-target]
Release Information	Statement introduced in Junos OS Release 8.4.
Description	Enable you to override the Layer 3 VPN import and export route targets used for importing and exporting routes for the MBGP MVPN network layer reachability information (NLRI).
Options	target <i>target-community</i> —Specify the export target community. unicast —Use the same target community as specified for unicast.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Export Target for an MBGP MVPN on page 15

family (VRF Advertisement)

Syntax	<code>family { inet-mvpn; inet6-mvpn; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> vrf-advertise-selective], [edit routing-instances <i>routing-instance-name</i> vrf-advertise-selective],
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Explicitly enable IPv4 or IPv6 MVPN routes to be advertised from the VRF instance while preventing all other route types from being advertised. The options are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring PIM-SSM GRE Selective Provider Tunnels on page 82 • inet-mvpn on page 124 • inet6-mvpn on page 125

group (Routing Instances)

Syntax	<pre> group address { source source-address { inter-region-segmented { fan-out fan-out value; threshold rate-value; } ldp-p2mp; pim-ssm { group-range multicast-prefix; } rsvp-te { label-switched-path-template { (default-template lsp-template-name); } static-lsp lsp-name; } threshold-rate number; } wildcard-source { inter-region-segmented { fan-out fan-out value; } ldp-p2mp; pim-ssm { group-range multicast-prefix; } rsvp-te { label-switched-path-template { (default-template lsp-template-name); } static-lsp lsp-name; } } } </pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective], [edit routing-instances <i>routing-instance-name</i> provider-tunnel selective]
Release Information	Statement introduced in Junos OS Release 8.5. The inter-region-segmented statement added in Junos OS Release 15.1.
Description	Specify the IP address for the multicast group configured for point-to-multipoint label-switched paths (LSPs) and PIM-SSM GRE selective provider tunnels.
Options	<p>address—Specify the IP address for the multicast group. This address must be a valid multicast group address.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Configuring the Multicast Group Address for an MBGP MVPN on page 79](#)
 - [Configuring PIM-SSM GRE Selective Provider Tunnels on page 82](#)

group-range (MBGP MVPN Tunnel)

Syntax	<code>group-range <i>multicast-prefix</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> source <i>source-address</i> pim-ssm],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> wildcard-source pim-ssm],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet wildcard-source pim-ssm],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6 wildcard-source pim-ssm],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> source <i>source-address</i> pim-ssm],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> wildcard-source pim-ssm],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet wildcard-source pim-ssm],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6 wildcard-source pim-ssm]</p>
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Establish the multicast group address range to use for creating MBGP MVPN source-specific multicast selective PMSI tunnels.
Options	<p><i>multicast-prefix</i>—Multicast group address range to be used to create MBGP MVPN source-specific multicast selective PMSI tunnels.</p> <p>Range: Any valid, nonreserved IPv4 multicast address range</p> <p>Default: None</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring PIM-SSM GRE Selective Provider Tunnels on page 82

group-rp-mapping

Syntax	<pre>group-rp-mapping { family (inet inet6) { log-interval <i>seconds</i>; maximum <i>limit</i>; threshold <i>value</i>; } log-interval <i>seconds</i>; maximum <i>limit</i>; threshold <i>value</i>; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp], [edit protocols pim rp], [edit routing-instances <i>routing-instance-name</i> protocols pim rp]</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure a limit for the number of incoming group-to-RP mappings.



NOTE: The maximum limit settings that you configure with the `maximum` and the `family (inet | inet6) maximum` statements are mutually exclusive. For example, if you configure a global maximum group-to-RP mapping limit, you cannot configure a limit at the family level for IPv4 or IPv6. If you attempt to configure a limit at both the global level and the family level, the device will not accept the configuration.

Options	<p>family (inet inet6)—(Optional) Specify either IPv4 or IPv6 messages to be counted towards the configured group-to-RP mapping limit.</p> <p>Default: Both IPv4 and IPv6 messages are counted towards the configured group-to-RP limit.</p> <p>The remaining statements are described separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring PIM State Limits on page 54

import-target

Syntax	<pre>import-target { target { target-value; receiver target-value; sender target-value; } unicast { receiver; sender; } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mvpn route-target], [edit routing-instances <i>routing-instance-name</i> protocols mvpn route-target]
Release Information	Statement introduced in Junos OS Release 8.4.
Description	Enable you to override the Layer 3 VPN import and export route targets used for importing and exporting routes for the MBGP MVPN NLRI.
Options	The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Import Target for an MBGP MVPN on page 16

inet-mvpn (BGP)

Syntax	<pre>inet-mvpn { signaling { accepted-prefix-limit { maximum <i>number</i>; teardown <i>percentage</i> { idle-timeout (forever <i>minutes</i>); } } damping; loops <i>number</i>; prefix-limit { maximum <i>number</i>; teardown <i>percentage</i> { idle-timeout (forever <i>minutes</i>); } } } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols bgp family], [edit protocols bgp family], [edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> family], [edit protocols bgp group <i>group-name</i> family]
Release Information	Statement introduced in Junos OS Release 8.4.
Description	Enable the <code>inet-mvpn</code> address family in BGP.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring NLRI Parameters for an MBGP MVPN on page 74

inet-mvpn (VRF Advertisement)

Syntax	inet-mvpn;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> vrf-advertise-selective family], [edit routing-instances <i>routing-instance-name</i> vrf-advertise-selective family]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Enable IPv4 MVPN routes to be advertised from the VRF instance.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Limiting Routes to Be Advertised by an MVPN VRF Instance on page 13

inet6-mvpn (BGP)

Syntax	<pre>inet6-mvpn { signaling { accepted-prefix-limit { maximum <i>number</i>; teardown <i>percentage</i> { idle-timeout (forever <i>minutes</i>); } } } loops <i>number</i> prefix-limit { maximum <i>number</i>; teardown <i>percentage</i> { idle-timeout (forever <i>minutes</i>); } } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols bgp family], [edit protocols bgp family], [edit logical-systems <i>logical-system-name</i> protocols bgp group <i>group-name</i> family], [edit protocols bgp group <i>group-name</i> family]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Enable the inet6-mvpn address family in BGP.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring NLRI Parameters for an MBGP MVPN on page 74 • BGP Feature Guide for Routing Devices

inet6-mvpn (VRF Advertisement)

Syntax	inet6-mvpn;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> vrf-advertise-selective family], [edit routing-instances <i>routing-instance-name</i> vrf-advertise-selective family],
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Enable IPv6 MVPN routes to be advertised from the VRF instance.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Limiting Routes to Be Advertised by an MVPN VRF Instance on page 13

ingress-replication

Syntax	<pre>ingress-replication { create-new-ucast-tunnel; label-switched-path { label-switched-path-template { (template-name default-template); } } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel],</p> <p>[edit protocols mvpn inter-region-template template <i>template-name</i> all-regions],</p> <p>[edit protocols mvpn inter-region-template template <i>template-name</i> region <i>region-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i>]</p>
Release Information	Statement introduced in Junos OS Release 10.4.
Description	<p>A provider tunnel type used for passing multicast traffic between routers through the MPLS cloud, or between PE routers when using MVPN. The ingress replication provider tunnel uses MPLS point-to-point LSPs to create the multicast distribution tree.</p> <p>Optionally, you can specify a label-switched path template. If you configure ingress-replication label-switched-path and do not include label-switched-path-template, ingress replication works with existing LDP or RSVP tunnels. If you include label-switched-path-template, the tunnels must be RSVP.</p>
Options	<p>create-new-ucast-tunnel—A new unicast tunnel to the destination that is created and used for ingress replication. The unicast tunnel is deleted later if the destination is no longer included in the multicast distribution tree. A template must be specified when and only when create-new-ucast-tunnel is included in the configuration..</p> <p>template-name—Name of the point-to-point LSP used for the new unicast tunnel.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Ingress Replication for IP Multicast Using MBGP MVPNs • Configuring Routing Instances for an MBGP MVPN on page 75 • create-new-ucast-tunnel on page 117 • mpls-internet-multicast on page 129

interface (Virtual Tunnel in Routing Instances)

Syntax	<pre>interface vt-<i>fpc/pic/port.unit-number</i> { multicast; primary; unicast; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	<p>In a multiprotocol BGP (MBGP) multicast VPN (MVPN), configure a virtual tunnel (VT) interface.</p> <p>VT interfaces are needed for multicast traffic on routing devices that function as combined provider edge (PE) and provider core (P) routers to optimize bandwidth usage on core links. VT interfaces prevent traffic replication when a P router also acts as a PE router (an exit point for multicast traffic).</p> <p>In an MBGP MVPN extranet, if there is more than one VRF routing instance on a PE router that has receivers interested in receiving multicast traffic from the same source, VT interfaces must be configured on all instances.</p> <p>Starting in Junos OS Release 12.3, you can configure multiple VT interfaces in each routing instance. This provides redundancy. A VT interface can be used in only one routing instance.</p>
Options	<p><i>vt-fpc/pic/port.unit-number</i>—Name of the VT interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Redundant Virtual Tunnel Interfaces in MBGP MVPNs</i> • <i>Example: Configuring MBGP MVPN Extranets</i>

label-switched-path-template (Multicast)

Syntax	<pre>label-switched-path-template { (default-template <i>lsp-template-name</i>); }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel rsvp-te],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel ingress-replication label-switched-path],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i> rsvp-te],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-options dynamic-tunnels <i>tunnel-name</i> rsvp-te <i>entry-name</i>],</p> <p>[edit protocols mvpn inter-region-segmented template <i>template-name</i> region <i>region-name</i> ingress-replication label-switched-path],</p> <p>[edit protocols mvpn inter-region-segmented template <i>template-name</i> region <i>region-name</i> rsvpe-te],</p> <p>[edit protocols mvpn inter-region-template template <i>template-name</i> all-regions ingress-replication label-switched-path],</p> <p>[edit protocols mvpn inter-region-template template <i>template-name</i> all-regions rsvp-te],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel ingress-replication label-switched-path],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel rsvp-te],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i> rsvp-te],</p> <p>[edit routing-options dynamic-tunnels <i>tunnel-name</i> rsvp-te <i>entry-name</i>]</p>
Release Information	Statement introduced in Junos OS Release 8.5.
Description	<p>Specify the LSP template. An LSP template is used as the basis for other dynamically generated LSPs. This feature can be used for a number of applications, including point-to-multipoint LSPs, flooding VPLS traffic, configuring ingress replication for IP multicast using MBGP MVPNs, and to enable RSVP automatic mesh. There is no default setting for the label-switched-path-template statement, so you must configure either the default-template using the default-template option, or you must specify the name of your preconfigured LSP template.</p>
Options	<p>default-template—Specify that the default LSP template be used for the dynamically generated LSPs.</p> <p><i>lsp-template-name</i>—Specify the name of an LSP to be used as a template for the dynamically generated LSPs.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Ingress Replication for IP Multicast Using MBGP MVPNs • Configuring RSVP-Signaled Inclusive Point-to-Multipoint LSPs for an MBGP MVPN on page 77

- *Flooding Unknown Traffic Using Point-to-Multipoint LSPs in VPLS*
- *Configuring RSVP Automatic Mesh*

mpls-internet-multicast

Syntax	mpls-internet-multicast;
Hierarchy Level	[edit routing-instances <i>routing-instance-name</i> instance-type] [edit protocols pim]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	<p>A nonforwarding routing instance type that supports Internet multicast over an MPLS network for the default master instance. No interfaces can be configured for it. Only one mpls-internet-multicast instance can be configured for each logical system.</p> <p>The mpls-internet-multicast configuration statement is also explicitly required under PIM in the master instance.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Ingress Replication for IP Multicast Using MBGP MVPNs</i> • ingress-replication on page 126

multicast (Virtual Tunnel in Routing Instances)

Syntax	multicast;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> interface vt- <i>fpc/pic/port.unit-number</i>], [edit routing-instances <i>routing-instance-name</i> interface vt- <i>fpc/pic/port.unit-number</i>]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	In a multiprotocol BGP (MBGP) multicast VPN (MVPN), configure the virtual tunnel (VT) interface to be used for multicast traffic only.
Default	If you omit this statement, the VT interface can be used for both multicast and unicast traffic.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring Redundant Virtual Tunnel Interfaces in MBGP MVPNs</i> • <i>Example: Configuring MBGP MVPN Extranets</i>

mvpn (NG-MVPN)

```
Syntax  mvpn {
        inter-region-template{
            template template-name {
                all-regions {
                    incoming;
                    ingress-replication {
                        create-new-ucast-tunnel;
                        label-switched-path {
                            label-switched-path-template (Multicast) {
                                (default-template | lsp-template-name);
                            }
                        }
                    }
                }
            }
            ldp-p2mp;
            rsvp-te {
                label-switched-path-template (Multicast) {
                    (default-template | lsp-template-name);
                }
            }
            static-lsp static-lsp;
            region region-name{
                incoming;
                ingress-replication {
                    create-new-ucast-tunnel;
                    label-switched-path {
                        label-switched-path-template (Multicast){
                            (default-template | lsp-template-name);
                        }
                    }
                }
            }
            ldp-p2mp;
            rsvp-te {
                label-switched-path-template (Multicast) {
                    (default-template | lsp-template-name);
                }
            }
            static-lsp static-lsp;
        }
    }
}

mvpn-mode (rpt-spt | spt-only);
receiver-site;
sender-site;
route-target {
    export-target {
        target target-community;
        unicast;
    }
    import-target {
        target {
            target-value;
            receiver target-value;
            sender target-value;
        }
    }
}
```

```
}  
    unicast {  
        receiver;  
        sender;  
    }  
}  
  
}  
  
traceoptions{  
    file filename <files number> <size size> <world-readable | no-world-readable>;  
    flag flag <flag-modifier> <disable>;  
}  
  
}
```

Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols], [edit protocols], [edit routing-instances <i>routing-instance-name</i> protocols]
Release Information	Statement introduced in Junos OS Release 8.4. Support for the traceoptions statement at the [edit protocols mvpn] hierarchy level introduced in Junos OS Release 13.3. Support for the inter-region-template statement at the [edit protocols mvpn] hierarchy level introduced in Junos OS Release 15.1.
Description	Configure next-generation multicast VPNs.
Options	receiver-site —Allow sites with multicast receivers. sender-site —Allow sites with multicast senders. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Routing Instances for an MBGP MVPN on page 75

mvpn-mode

Syntax	<code>mvpn-mode (rpt-spt spt-only);</code>
Hierarchy Level	[edit logical-systems <i>profile-name</i> routing-instances <i>instance-name</i> protocols mvpn], [edit routing-instances <i>instance-name</i> protocols mvpn]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Configure the mode for customer PIM (C-PIM) join messages. The remaining statements are explained separately.
Default	spt-only
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 49• Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 47

pim-asm

Syntax	<pre>pim-asm { group-address <i>address</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel], [edit routing-instances <i>routing-instance-name</i> provider-tunnel]
Release Information	Statement introduced in Junos OS Release 8.3.
Description	Specify a Protocol Independent Multicast (PIM) sparse mode provider tunnel for an MBGP MVPN or for a draft-rosen MVPN. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring PIM Provider Tunnels for an MBGP MVPN on page 82

pim-ssm (Selective Tunnel)

Syntax	<pre>pim-ssm { group-range <i>multicast-prefix</i>; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> source <i>source-address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> wildcard-source],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet wildcard-source],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6 wildcard-source],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> source <i>source-address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> wildcard-source],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet wildcard-source],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6 wildcard-source]</p>
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Establish the multicast group address range to use for creating MBGP MVPN source-specific multicast selective PMSI tunnels.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring PIM-SSM GRE Selective Provider Tunnels on page 82

primary (Virtual Tunnel in Routing Instances)

Syntax	<code>primary;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> interface <i>vt-fpc/pic/port.unit-number</i>], [edit routing-instances <i>routing-instance-name</i> interface <i>vt-fpc/pic/port.unit-number</i>]
Release Information	Statement introduced in Junos OS Release 12.3.
Description	<p>In a multiprotocol BGP (MBGP) multicast VPN (MVPN), configure the virtual tunnel (VT) interface to be used as the primary interface for multicast traffic.</p> <p>Junos OS supports up to eight VT interfaces configured for multicast in a routing instance to provide redundancy for MBGP (next-generation) MVPNs. This support is for RSVP point-to-multipoint provider tunnels as well as multicast Label Distribution Protocol (MLDP) provider tunnels. This feature works for extranets as well.</p> <p>This statement allows you to configure one of the VT interfaces to be the primary interface, which is always used if it is operational. If a VT interface is configured as the primary, it becomes the nexthop that is used for traffic coming in from the core on the label-switched path (LSP) into the routing instance. When a VT interface is configured to be primary and the VT interface is used for both unicast and multicast traffic, only the multicast traffic is affected.</p> <p>If no VT interface is configured to be the primary or if the primary VT interface is unusable, one of the usable configured VT interfaces is chosen to be the nexthop that is used for traffic coming in from the core on the LSP into the routing instance. If the VT interface in use goes down for any reason, another usable configured VT interface in the routing instance is chosen. When the VT interface in use changes, all multicast routes in the instance also switch their reverse-path forwarding (RPF) interface to the new VT interface to allow the traffic to be received.</p> <p>To realize the full benefit of redundancy, we recommend that when you configure multiple VT interfaces, at least one of the VT interfaces be on a different Tunnel PIC from the other VT interfaces. However, Junos OS does not enforce this.</p>
Default	If you omit this statement, Junos OS chooses a VT interface to be the active interface for multicast traffic.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> <i>Example: Configuring Redundant Virtual Tunnel Interfaces in MBGP MVPNs</i> <i>Example: Configuring MBGP MVPN Extranets</i>

provider-tunnel

```

Syntax  provider-tunnel {
        ingress-replication {
            create-new-ucast-tunnel;
            label-switched-path-template {
                (default-template | lsp-template-name);
            }
        }
        ldp-p2mp;
        pim-asm {
            group-address address;
        }
        mdt {
            data-mdt-reuse;
            group-range multicast-prefix;
            threshold {
                group group-address {
                    source source-address {
                        rate threshold-rate;
                    }
                }
            }
            tunnel-limit limit;
        }
    }
    pim-ssm {
        group-address address;
    }
    rsvp-te {
        label-switched-path-template {
            (default-template | lsp-template-name);
        }
        static-lsp lsp-name;
    }
    selective {
        group multicast--prefix/prefix-length {
            source ip--prefix/prefix-length {
                ldp-p2mp;
                create-new-ucast-tunnel;
                label-switched-path-template {
                    (default-template | lsp-template-name);
                }
            }
        }
        pim-ssm {
            group-range multicast-prefix;
        }
        rsvp-te {
            label-switched-path-template {
                (default-template | lsp-template-name);
            }
            static-lsp point-to-multipoint-lsp-name;
        }
        threshold-rate kbps;
    }
}

```

```


wildcard-source {
  pim-ssm {
    group-range multicast-prefix;
  }
  rsvp-te {
    label-switched-path-template {
      (default-template | lsp-template-name);
    }
    static-lsp point-to-multipoint-lsp-name;
  }
  threshold-rate kpbs;
}
}
tunnel-limit number;
wildcard-group-inet {
  wildcard-source {
    pim-ssm {
      group-range multicast-prefix;
    }
    rsvp-te {
      label-switched-path-template {
        (default-template | lsp-template-name);
      }
      static-lsp lsp-name;
    }
    threshold-rate number;
  }
}
wildcard-group-inet6 {
  wildcard-source {
    pim-ssm {
      group-range multicast-prefix;
    }
    rsvp-te {
      label-switched-path-template {
        (default-template | lsp-template-name);
      }
      static-lsp lsp-name;
    }
    threshold-rate number;
  }
}
}
}

```

Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced in Junos OS Release 8.3. The selective statement and substatements added in Junos OS Release 8.5. The ingress-replication statement and substatements added in Junos OS Release 10.4.
Description	Configure virtual private LAN service (VPLS) flooding of unknown unicast, broadcast, and multicast traffic using point-to-multipoint LSPs. Also configure point-to-multipoint LSPs for MBGP MVPNs.

Options	The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Flooding Unknown Traffic Using Point-to-Multipoint LSPs in VPLS</i>• Configuring RSVP-Signaled Inclusive Point-to-Multipoint LSPs for an MBGP MVPN on page 77• <i>Example: Configuring Data MDTs and Provider Tunnels Operating in Source-Specific Multicast Mode</i>

register-limit

Syntax	<pre> register-limit { family (inet inet6) { log-interval <i>seconds</i>; maximum <i>limit</i>; threshold <i>value</i>; } log-interval <i>seconds</i>; maximum <i>limit</i>; threshold <i>value</i>; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim rp],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim rp],</p> <p>[edit protocols pim rp],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim rp]</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure a limit for the number of incoming (S,G) PIM registers.
<div>  <p>NOTE: The maximum limit settings that you configure with the <code>maximum</code> and the <code>family (inet inet6) maximum</code> statements are mutually exclusive. For example, if you configure a global maximum PIM register message limit, you cannot configure a limit at the family level for IPv4 or IPv6. If you attempt to configure a limit at both the global level and the family level, the device will not accept the configuration.</p> </div>	
Options	<p>family (inet inet6)—(Optional) Specify either IPv4 or IPv6 messages to be counted towards the configured register message limit.</p> <p>Default: Both IPv4 and IPv6 messages are counted towards the configured register message limit.</p> <p>The remaining statements are described separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring PIM State Limits on page 54 • <code>clear pim join</code> • <code>clear pim register</code>


route-target (Protocols MVPN)

Syntax	<pre> route-target { export-target { target <i>target-community</i>; unicast; } import-target { target { <i>target-value</i>; receiver <i>target-value</i>; sender <i>target-value</i>; } unicast { receiver; sender; } } } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mvpn],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols mvpn]</p>
Release Information	Statement introduced in Junos OS Release 8.4.
Description	Enable you to override the Layer 3 VPN import and export route targets used for importing and exporting routes for the MBGP MVPN NLRI.
Default	The multicast VPN routing instance uses the import and export route targets configured for the Layer 3 VPN.
Options	The remaining statements are explained separately.
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring VRF Route Targets for Routing Instances for an MBGP MVPN on page 14

rpt-spt

Syntax	rpt-spt;
Hierarchy Level	[edit logical-systems <i>profile-name</i> routing-instances <i>instance-name</i> protocols mvpn mvpn-mode], [edit routing-instances <i>instance-name</i> protocols mvpn mvpn-mode]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Use rendezvous-point trees for customer PIM (C-PIM) join messages, and switch to the shortest-path tree after the source is known.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Shared-Tree Data Distribution Across Provider Cores for Providers of MBGP MVPNs on page 49

rsvp-te (Routing Instances Provider Tunnel Selective)

Syntax	<pre> rsvp-te { label-switched-path-template { (default-template <i>lsp-template-name</i>); } static-lsp <i>lsp-name</i>; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> wildcard-source],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet wildcard-source],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6 wildcard-source],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i>]</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> wildcard-source],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet wildcard-source],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6 wildcard-source]</p>
Release Information	Statement introduced in Junos OS Release 8.5.
Description	<p>Configure the properties of the RSVP traffic-engineered point-to-multipoint LSP for MBGP MVPNs.</p> <p>The remaining statements are explained separately.</p>
	<div>  <p>NOTE: Junos OS Release 11.2 and earlier do not support point-to-multipoint LSPs with next-generation multicast VPNs on MX80 routers.</p> </div>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Selective Provider Tunnels for an MBGP MVPN on page 78

selective

```
Syntax  selective {
    group multicast-prefix/prefix-length {
        source ip-prefix/prefix-length {
            ingress-replication {
                create-new-ucast-tunnel;
                label-switched-path-template {
                    (default-template | lsp-template-name);
                }
            }
            ldp-p2mp;
            pim-ssm {
                group-range multicast-prefix;
            }
            rsvp-te {
                label-switched-path-template {
                    (default-template | lsp-template-name);
                }
                static-lsp point-to-multipoint-lsp-name;
            }
            threshold-rate kbits;
        }
        wildcard-source {
            ldp-p2mp;
            pim-ssm {
                group-range multicast-prefix;
            }
            rsvp-te {
                label-switched-path-template {
                    (default-template | lsp-template-name);
                }
            }
            static-lsp point-to-multipoint-lsp-name;
            threshold-rate kbits;
        }
    }
    tunnel-limit number;
    wildcard-group-inet {
        wildcard-source {
            ldp-p2mp;
            pim-ssm {
                group-range multicast-prefix;
            }
            rsvp-te {
                label-switched-path-template {
                    (default-template | lsp-template-name);
                }
            }
            static-lsp lsp-name;
        }
        threshold-rate number;
    }
}
```


```

wildcard-group-inet6 {
  wildcard-source {
    ldp-p2mp;
    pim-ssm {
      group-range multicast-prefix;
    }
    rsvp-te {
      label-switched-path-template {
        (default-template | lsp-template-name);
      }
      static-lsp lsp-name;
    }
    threshold-rate number;
  }
}

```

Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel], [edit routing-instances <i>routing-instance-name</i> provider-tunnel]
Release Information	Statement introduced in Junos OS Release 8.5. The ingress-replication statement and substatements added in Junos OS Release 10.4.
Description	Configure selective point-to-multipoint LSPs for an MBGP MVPN. Selective point-to-multipoint LSPs send traffic only to the receivers configured for the MBGP MVPNs, helping to minimize flooding in the service provider's network. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Selective Provider Tunnels for an MBGP MVPN on page 78 • Configuring PIM-SSM GRE Selective Provider Tunnels on page 82

sglimit

Syntax	<pre>sglimit { family (inet inet6) { log-interval <i>seconds</i>; maximum <i>limit</i>; threshold <i>value</i>; } log-interval <i>seconds</i>; maximum <i>limit</i>; threshold <i>value</i>; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols pim],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols pim],</p> <p>[edit protocols pim],</p> <p>[edit routing-instances <i>routing-instance-name</i> protocols pim]</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure a limit for the number of accepted (*G) and (S,G) PIM join states.
<div>  <p>NOTE: The maximum limit settings that you configure with the maximum and the family (inet inet6) maximum statements are mutually exclusive. For example, if you configure a global maximum PIM join state limit, you cannot configure a limit at the family level for IPv4 or IPv6 joins. If you attempt to configure a limit at both the global level and the family level, the device will not accept the configuration.</p> </div>	
Options	<p>family (inet inet6)—(Optional) Specify either IPv4 or IPv6 join states to be counted towards the configured join state limit.</p> <p>Default: Both IPv4 and IPv6 join states are counted towards the configured join state limit.</p> <p>The remaining statements are described separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring PIM State Limits on page 54 • <code>clear pim join</code>

source (Routing Instances Provider Tunnel Selective)

Syntax	<pre> source <i>source-address</i> { ldp-p2mp; pim-ssm { group-range <i>multicast-prefix</i>; } rsvp-te { label-switched-path-template { (default-template <i>lsp-template-name</i>); } static-lsp <i>lsp-name</i>; } threshold-rate <i>number</i>; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i>]</p>
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the IP address for the multicast source. This statement is a part of the point-to-multipoint LSP and PIM-SSM GRE selective provider tunnel configuration for MBGP MVPNs.
Options	<p><i>source-address</i>—IP address for the multicast source.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Multicast Source Address for an MBGP MVPN on page 80 • Configuring PIM-SSM GRE Selective Provider Tunnels on page 82

spt-only

Syntax	spt-only;
Hierarchy Level	[edit logical-systems <i>profile-name</i> routing-instances <i>instance-name</i> protocols mvpn mvpn-mode], [edit routing-instances <i>instance-name</i> protocols mvpn mvpn-mode]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Set the MVPN mode to learn about active multicast sources using multicast VPN source-active routes. This is the default mode.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring SPT-Only Mode for Multiprotocol BGP-Based Multicast VPNs on page 47

static-lsp

Syntax	static-lsp <i>lsp-name</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel rsvp-te], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i> rsvp-te], [edit routing-instances <i>routing-instance-name</i> provider-tunnel rsvp-te], [edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i> rsvp-te]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the name of the static point-to-multipoint LSP used for an MBGP MVPN. Use this statement to specify the static LSP for both inclusive and selective point-to-multipoint LSPs.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Selective Provider Tunnels for an MBGP MVPN on page 78

target (Routing Instances MVPN)

Syntax	<code>target <i>target-value</i> { receiver <i>target-value</i>; sender <i>target-value</i>; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mvpn route-target import-target], [edit routing-instances <i>routing-instance-name</i> protocols mvpn route-target import-target]
Release Information	Statement introduced in Junos OS Release 8.4.
Description	Specify the target value when importing sender and receiver site routes.
Options	<p><i>target-value</i>—Specify the target value when importing sender and receiver site routes.</p> <p><i>receiver</i>—Specify the target community used when importing receiver site routes.</p> <p><i>sender</i>—Specify the target community used when importing sender site routes.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Import Target Receiver and Sender for an MBGP MVPN on page 16

threshold-rate

Syntax	<code>threshold-rate <i>kbps</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-address</i> wildcard-source],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet wildcard-source],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6 wildcard-source],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> source <i>source-address</i>]</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>address</i> wildcard-source]</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet wildcard-source],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6 wildcard-source]</p>
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the data threshold required before a new tunnel is created for a dynamic selective point-to-multipoint LSP. This statement is part of the configuration for point-to-multipoint LSPs for MBGP MVPNs and PIM-SSM GRE or RSVP-TE selective provider tunnels.
Options	<p><i>number</i>—Specify the data threshold required before a new tunnel is created.</p> <p>Range: 0 through 1,000,000 kilobits per second. Specifying 0 is equivalent to not including the statement.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Threshold for Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 81 • Configuring PIM-SSM GRE Selective Provider Tunnels on page 82

traceoptions (Protocols MVPN)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i> <<i>flag-modifier</i>> <disable>; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols mvpn], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mvpn], [edit protocols mvpn], [edit routing-instances <i>routing-instance-name</i> protocols mvpn]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.4. Support at the [edit protocols mvpn] hierarchy level introduced in Junos OS Release 13.3.</p>
Description	Trace traffic flowing through a Multicast BGP (MBGP) MVPN.
Options	<p>disable—(Optional) Disable the tracing operation. You can use this option to disable a single operation when you have defined a broad group of tracing operations, such as all.</p> <p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" ").</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches this size, it is renamed <i>trace-file.0</i>. When <i>trace-file</i> again reaches its maximum size, <i>trace-file.0</i> is renamed <i>trace-file.1</i> and <i>trace-file</i> is renamed <i>trace-file.0</i>. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000 files Default: 2 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can specify any of the following flags:</p> <ul style="list-style-type: none"> • all—All multicast VPN tracing options • cmcast-join—Multicast VPN C-multicast join routes • error—Error conditions • general—General events • inter-as-ad—Multicast VPN inter-AS automatic discovery routes • intra-as-ad—Multicast VPN intra-AS automatic discovery routes • leaf-ad—Multicast VPN leaf automatic discovery routes • mdt-safi-ad—Multicast VPN MDT SAFI automatic discovery routes

- **nlri**—Multicast VPN advertisements received or sent by means of the BGP
- **normal**—Normal events
- **policy**—Policy processing
- **route**—Routing information
- **source-active**—Multicast VPN source active routes
- **spmsi-ad**—Multicast VPN SPMSI auto discovery active routes
- **state**—State transitions
- **task**—Routing protocol task processing
- **timer**—Routing protocol timer processing
- **tunnel**—Provider tunnel events
- **umh**—Upstream multicast hop (UMH) events

flag-modifier—(Optional) Modifier for the tracing flag. You can specify the following modifiers:

- **detail**—Provide detailed trace information
- **disable**—Disable the tracing flag
- **receive**—Trace received packets
- **send**—Trace sent packets

no-world-readable—Do not allow any user to read the log file.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **xk** to specify kilobytes, **xm** to specify megabytes, or **xg** to specify gigabytes

Range: 10 KB through the maximum file size supported on your system

Default: 1 MB

world-readable—Allow any user to read the log file.

Required Privilege Level	routing—To view this statement in the configuration.
	routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Tracing MBGP MVPN Traffic and Operations on page 101

tunnel-limit (Routing Instances Provider Tunnel Selective)

Syntax	tunnel-limit <i>number</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective], [edit routing-instances <i>routing-instance-name</i> provider-tunnel selective]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify a limit on the number of selective tunnels that can be created for an LSP. This limit can be applied to the following types of selective tunnels: <ul style="list-style-type: none"> • Ingress replication tunnels • LDP-signaled LSP • LDP point-to-multipoint LSP • PIM-SSM provider tunnel • RSVP-signaled LSP • RSVP-signaled point-to-multipoint LSP
Options	<i>number</i> —Specify the tunnel limit. Range: 0 through 1024
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Tunnel Limit for Dynamic Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 81 • selective on page 142 • wildcard-source on page 156

unicast (Route Target Community)

Syntax	<code>unicast { receiver; sender; }</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols mvpn route-target import-target], [edit routing-instances <i>routing-instance-name</i> protocols mvpn route-target import-target]
Release Information	Statement introduced in Junos OS Release 8.4.
Description	Specify the same target community configured for unicast.
Options	receiver —Specify the unicast target community used when importing receiver site routes. sender —Specify the unicast target community used when importing sender site routes.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Import Target Unicast Parameters for an MBGP MVPN on page 17

unicast (Virtual Tunnel in Routing Instances)

Syntax	<code>unicast;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> interface <i>vt-fpc/pic/port.unit-number</i>], [edit routing-instances <i>routing-instance-name</i> interface <i>vt-fpc/pic/port.unit-number</i>]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	In a multiprotocol BGP (MBGP) multicast VPN (MVPN), configure the virtual tunnel (VT) interface to be used for unicast traffic only.
Default	If you omit this statement, the VT interface can be used for both multicast and unicast traffic.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Redundant Virtual Tunnel Interfaces in MBGP MVPNs• Example: Configuring MBGP MVPN Extranets

vrf-advertise-selective

Syntax	<pre>vrf-advertise-selective { family { inet-mvpn; inet6-mvpn; } }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1. Statement introduced in Junos OS Release 12.3 for ACX Series routers.
Description	<p>Explicitly enable IPv4 or IPv6 MVPN routes to be advertised from the VRF instance while preventing all other route types from being advertised.</p> <p>If you configure the vrf-advertise-selective statement without any of its options, the router or switch has the same behavior as if you configured the no-vrf-advertise statement. All VPN routes are prevented from being advertised from a VRF routing instance to the remote PE routers. This behavior is useful for hub-and-spoke configurations, enabling you to configure a PE router to not advertise VPN routes from the primary (hub) instance. Instead, these routes are advertised from the secondary (downstream) instance.</p> <p>The options are explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Limiting Routes to Be Advertised by an MVPN VRF Instance on page 13 • <i>no-vrf-advertise</i>

wildcard-group-inet

Syntax	<pre> wildcard-group-inet { wildcard-source { inter-region-segmented { fan-out <i>fan-out value</i>; } ldp-p2mp; pim-ssm { group-range <i>multicast-prefix</i>; } rsvp-te { label-switched-path-template { (default-template <i>lsp-template-name</i>); } static-lsp <i>lsp-name</i>; } threshold-rate <i>number</i>; } } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>The inter-region-segmented statement added in Junos OS Release 15.1.</p>
Description	<p>Configure a wildcard group matching any group IPv4 address.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • wildcard-group-inet6 on page 155 • Example: Configuring Selective Provider Tunnels Using Wildcards on page 73 • Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 67 • Configuring a Selective Provider Tunnel Using Wildcards on page 72

wildcard-group-inet6

Syntax	<pre>wildcard-group-inet6 { wildcard-source { inter-region-segmented{ fan-out <i>fan-out value</i>; } ldp-p2mp; pim-ssm { group-range <i>multicast-prefix</i>; } rsvp-te { label-switched-path-template { (default-template <i>lsp-template-name</i>); } static-lsp <i>lsp-name</i>; } threshold-rate <i>number</i>; } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>The inter-region-segmented statement added in Junos OS Release 15.1.</p>
Description	<p>Configure a wildcard group matching any group IPv6 address.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • wildcard-group-inet on page 154 • Example: Configuring Selective Provider Tunnels Using Wildcards on page 73 • Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 67 • Configuring a Selective Provider Tunnel Using Wildcards on page 72

wildcard-source (Selective Provider Tunnels)

Syntax	<pre> wildcard-source { inter-region-segmented { fan-out <i>fan-out value</i>; } ldp-p2mp; pim-ssm { group-range <i>multicast-prefix</i>; } rsvp-te { label-switched-path-template { (default-template <i>lsp-template-name</i>); } } static-lsp <i>lsp-name</i>; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-prefix</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective group <i>group-prefix</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet],</p> <p>[edit routing-instances <i>routing-instance-name</i> provider-tunnel selective wildcard-group-inet6]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>The inter-region-segmented statement added in Junos OS Release 15.1.</p>
Description	<p>Configure a selective provider tunnel for a shared tree using a wildcard source.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • wildcard-group-inet on page 154 • wildcard-group-inet6 on page 155 • Example: Configuring Selective Provider Tunnels Using Wildcards on page 73 • Understanding Wildcards to Configure Selective Point-to-Multipoint LSPs for an MBGP MVPN on page 67 • Configuring a Selective Provider Tunnel Using Wildcards on page 72

CHAPTER 11

Operational Commands

- [Operational-Mode Commands on page 157](#)

Operational-Mode Commands

- [Overview of Junos OS CLI Operational Mode Commands on page 157](#)
- [Example: Running Operational Mode Commands on Logical Systems on page 160](#)
- [Example: Viewing BGP Trace Files on Logical Systems on page 161](#)
- [Example: Configuring System Logging on Logical Systems on page 166](#)

Overview of Junos OS CLI Operational Mode Commands

This topic provides an overview of Junos OS CLI operational mode commands and contains the following sections:

- [CLI Command Categories on page 157](#)
- [Commonly Used Operational Mode Commands on page 158](#)

CLI Command Categories

When you log in to a device running Junos OS and the CLI starts, there are several broad groups of CLI commands:

- Commands for controlling the CLI environment—Some set commands in the **set** hierarchy configure the CLI display screen. For information about these commands, see *Understanding the Junos OS CLI Modes, Commands, and Statement Hierarchies*.
- Commands for monitoring and troubleshooting—The following commands display information and statistics about the software and test network connectivity. Detailed command descriptions are provided in the *Junos OS Interfaces Command Reference*.
 - **clear**—Clear statistics and protocol database information.
 - **mtrace**—Trace mtrace packets from source to receiver.
 - **monitor**—Perform real-time debugging of various software components, including the routing protocols and interfaces.
 - **ping**—Determine the reachability of a remote network host.

- **show**—Display the current configuration and information about interfaces, routing protocols, routing tables, routing policy filters, system alarms, and the chassis.
- **test**—Test the configuration and application of policy filters and autonomous system (AS) path regular expressions.
- **traceroute**—Trace the route to a remote network host.
- Commands for connecting to other network systems—The **ssh** command opens Secure Shell connections, and the **telnet** command opens telnet sessions to other hosts on the network. For information about these commands, see the [CLI Explorer](#).
- Commands for copying files—The **copy** command copies files from one location on the router or switch to another, from the router or switch to a remote system, or from a remote system to the router or switch. For information about these commands, see the [CLI Explorer](#).
- Commands for restarting software processes—The commands in the **restart** hierarchy restart the various Junos OS processes, including the routing protocol, interface, and SNMP. For information about these commands, see the [CLI Explorer](#).
- A command—**request**—for performing system-level operations, including stopping and rebooting the router or switch and loading Junos OS images. For information about this command, see the [CLI Explorer](#).
- A command—**start**—to exit the CLI and start a UNIX shell. For information about this command, see the [CLI Explorer](#).
- A command—**configure**—for entering configuration mode, which provides a series of commands that configure Junos OS, including the routing protocols, interfaces, network management, and user access. For information about the CLI configuration commands, see *Understanding Junos OS CLI Configuration Mode*.
- A command—**quit**—to exit the CLI. For information about this command, see the [CLI Explorer](#).
- For more information about the CLI operational mode commands, see the [CLI Explorer](#).

Commonly Used Operational Mode Commands

Table 4 on page 158 lists some operational commands you may find useful for monitoring router or switch operation. For a complete description of operational commands, see the Junos OS command references.



NOTE: The QFX3500 switch does not support the IS-IS, OSPF, BGP, MPLS, and RSVP protocols.

Table 4: Commonly Used Operational Mode Commands

Items to Check	Description	Command
Software version	Versions of software running on the router or switch	show version

Table 4: Commonly Used Operational Mode Commands (*continued*)

Items to Check	Description	Command
Log files	Contents of the log files	monitor
	Log files and their contents and recent user logins	show log
Remote systems	Host reachability and network connectivity	ping
	Route to a network system	tracert
Configuration	Current system configuration	show configuration
Manipulate files	List of files and directories on the router or switch	file list
	Contents of a file	file show
Interface information	Detailed information about interfaces	show interfaces
Chassis	Chassis alarm status	show chassis alarms
	Information currently on craft display	show chassis craft-interface
	Router or switch environment information	show chassis environment
	Hardware inventory	show chassis hardware
Routing table information	Information about entries in the routing tables	show route
Forwarding table information	Information about data in the kernel's forwarding table	show route forwarding-table
IS-IS	Adjacent routers or switches	show isis adjacency
OSPF	Display standard information about OSPF neighbors	show ospf neighbor
BGP	Display information about BGP neighbors	show bgp neighbor
MPLS	Status of interfaces on which MPLS is running	show mpls interface
	Configured LSPs on the router or switch, as well as all ingress, transit, and egress LSPs	show mpls lsp
	Routes that form a label-switched path	show route label-switched-path
RSVP	Status of interfaces on which RSVP is running	show rsvp interface
	Currently active RSVP sessions	show rsvp session
	RSVP packet and error counters	show rsvp statistics

Example: Running Operational Mode Commands on Logical Systems

This example shows how to set the CLI to a specified logical system view, run operational-mode commands for the logical system, and then return to the main router view.

- [Requirements on page 160](#)
- [Overview on page 160](#)
- [Configuration on page 160](#)

Requirements

You must have the **view** privilege for the logical system.

Overview

For some operational-mode commands, you can include a **logical-system** option to narrow the output of the command or to limit the operation of the command to the specified logical system. For example, the **show route** command has a **logical-system** option. To run this command on a logical system called LS3, you can use **show route logical-system LS3**. However, some commands, such as **show interfaces**, do not have a **logical-system** option. For commands like this, you need another approach.

You can place yourself into the context of a specific logical system. To configure a logical system context, issue the **set cli logical-system logical-system-name** command.

When the CLI is in logical system context mode and you enter an operational-mode command, the output of the command displays information related to the logical system only.

Configuration

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To set the CLI to a specific logical system context:

1. From the main router, configure the logical system.

```
[edit]
user@host# set logical-systems LS3
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
user@host# exit
```

3. Set the CLI to view the logical system.

```
user@host> set cli logical-system LS3
Logical system: LS3
user@host:LS3>
```


- Run an operational-mode command.

```
user@host:LS3> show interfaces terse
Interface           Admin Link Proto  Local           Remote
lt-1/2/0
lt-1/2/0.3           up    up    inet   10.0.2.1/30
```

- Enter configuration mode to edit the logical system configuration.

```
user@host:LS3> edit
Entering configuration mode
```

```
user@host:LS3#
```

- Exit configuration mode to return to operational mode.

```
user@host:LS3# exit
Exiting configuration mode
```

- Clear the logical system view to return to the main router view.

```
user@host:LS3> clear cli logical-system
Cleared default logical system
```

```
user@host>
```

- To achieve the same effect when using a Junos XML protocol client application, include the `<set-logical-system>` tag.

```
<rpc>
<set-logical-system>
<logical-system>LS1</logical-system>
</set-logical-system>
</rpc>
```

Example: Viewing BGP Trace Files on Logical Systems

This example shows how to list and view files that are stored on a logical system.

- [Requirements on page 161](#)
- [Overview on page 162](#)
- [Configuration on page 162](#)
- [Verification on page 166](#)

Requirements

- You must have the **view** privilege for the logical system.
- Configure a network, such as the BGP network shown in *Example: Configuring Internal BGP Peering Sessions on Logical Systems*.

Overview

Logical systems have their individual directory structure created in the `/var/logical-systems/logical-system-name` directory. It contains the following subdirectories:

- `/config`—Contains the active configuration specific to the logical system.
- `/log`—Contains system log and tracing files specific to the logical system.

To maintain backward compatibility for the log files with previous versions of Junos OS, a symbolic link (symlink) from the `/var/logs/logical-system-name` directory to the `/var/logical-systems/logical-system-name` directory is created when a logical system is configured.

- `/tmp`—Contains temporary files specific to the logical system.

The file system for each logical system enables logical system users to view trace logs and modify logical system files. Logical system administrators have full access to view and modify all files specific to the logical system.

Logical system users and administrators can save and load configuration files at the logical-system level using the **save** and **load** configuration mode commands. In addition, they can also issue the **show log**, **monitor**, and **file** operational mode commands at the logical-system level.

This example shows how to configure and view a BGP trace file on a logical system. The steps can be adapted to apply to trace operations for any Junos OS hierarchy level that supports trace operations.



TIP: To view a list of hierarchy levels that support tracing operations, enter the `help apropos traceoptions` command in configuration mode.

Configuration

- [Configuring Trace Operations on page 163](#)
- [Viewing the Trace File on page 163](#)
- [Deactivating and Reactivating Trace Logging on page 165](#)
- [Results on page 166](#)

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set logical-systems A protocols bgp group internal-peers traceoptions file bgp-log
set logical-systems A protocols bgp group internal-peers traceoptions file size 10k
set logical-systems A protocols bgp group internal-peers traceoptions file files 2
set logical-systems A protocols bgp group internal-peers traceoptions flag update detail
```

Configuring Trace Operations

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure the trace operations:

1. Configure trace operations on the logical system.

```
[edit logical-systems A protocols bgp group internal-peers]
user@host# set traceoptions file bgp-log
user@host# set traceoptions file size 10k
user@host# set traceoptions file files 2
user@host# set traceoptions flag update detail
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
```

Viewing the Trace File

Step-by-Step Procedure To view the trace file:

1. In operational mode on the main router, list the directories on the logical system.

```
user@host> file list /var/logical-systems/A
/var/logical-systems/A:
config/
log/
tmp/
```

2. In operational mode on the main router, list the log files on the logical system.

```
user@host> file list /var/logical-systems/A/log/
/var/logical-systems/A/log:
bgp-log
```

3. View the contents of the **bgp-log** file.

```
user@host> file show /var/logical-systems/A/log/bgp-log
Aug 10 17:12:01 trace_on: Tracing to "/var/log/A/bgp-log" started
Aug 10 17:14:22.826182 bgp_peer_mgmt_clear:5829: NOTIFICATION sent to
192.163.6.4 (Internal AS 17): code 6 (Cease) subcode 4 (Administratively
Reset), Reason: Management session cleared BGP neighbor
Aug 10 17:14:22.826445 bgp_send: sending 21 bytes to 192.163.6.4 (Internal
AS 17)
Aug 10 17:14:22.826499
Aug 10 17:14:22.826499 BGP SEND 192.168.6.5+64965 -> 192.163.6.4+179
Aug 10 17:14:22.826559 BGP SEND message type 3 (Notification) length 21
Aug 10 17:14:22.826598 BGP SEND Notification code 6 (Cease) subcode 4
(Administratively Reset)
Aug 10 17:14:22.831756 bgp_peer_mgmt_clear:5829: NOTIFICATION sent to
192.168.40.4 (Internal AS 17): code 6 (Cease) subcode 4 (Administratively
Reset), Reason: Management session cleared BGP neighbor
Aug 10 17:14:22.831851 bgp_send: sending 21 bytes to 192.168.40.4 (Internal
AS 17)
Aug 10 17:14:22.831901
Aug 10 17:14:22.831901 BGP SEND 192.168.6.5+53889 -> 192.168.40.4+179
```

```
Aug 10 17:14:22.831959 BGP SEND message type 3 (Notification) length 21
Aug 10 17:14:22.831999 BGP SEND Notification code 6 (Cease) subcode 4
(Administratively Reset)
...
```

4. Filter the output of the log file.

```
user@host> file show /var/logical-systems/A/log/bgp-log | match "flags 0x40"
Aug 10 17:14:54.867460 BGP SEND flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.867595 BGP SEND flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.867650 BGP SEND flags 0x40 code NextHop(3): 192.168.6.5
Aug 10 17:14:54.867692 BGP SEND flags 0x40 code LocalPref(5): 100
Aug 10 17:14:54.884529 BGP RECV flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.884581 BGP RECV flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.884628 BGP RECV flags 0x40 code NextHop(3): 192.168.6.4
Aug 10 17:14:54.884667 BGP RECV flags 0x40 code LocalPref(5): 100
Aug 10 17:14:54.911377 BGP RECV flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.911422 BGP RECV flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.911466 BGP RECV flags 0x40 code NextHop(3): 192.168.40.4
Aug 10 17:14:54.911507 BGP RECV flags 0x40 code LocalPref(5): 100
Aug 10 17:14:54.916008 BGP SEND flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.916054 BGP SEND flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.916100 BGP SEND flags 0x40 code NextHop(3): 192.168.6.5
Aug 10 17:14:54.916143 BGP SEND flags 0x40 code LocalPref(5): 100
Aug 10 17:14:54.920304 BGP RECV flags 0x40 code Origin(1): IGP
Aug 10 17:14:54.920348 BGP RECV flags 0x40 code ASPath(2) length 0: <null>
Aug 10 17:14:54.920393 BGP RECV flags 0x40 code NextHop(3): 10.0.0.10
Aug 10 17:14:54.920434 BGP RECV flags 0x40 code LocalPref(5): 100
```

5. View the tracing operations in real time.

```
user@host> clear bgp neighbor logical-system A
Cleared 2 connections
```



CAUTION: Clearing the BGP neighbor table is disruptive in a production environment.

6. Run the **monitor start** command with an optional **match** condition.

```
user@host> monitor start A/bgp-log | match 0.0.0.0/0
Aug 10 19:21:40.773467 BGP RECV          0.0.0.0/0
Aug 10 19:21:40.773685 bgp_rcv_nlrri: 0.0.0.0/0
Aug 10 19:21:40.773778 bgp_rcv_nlrri: 0.0.0.0/0 belongs to meshgroup
Aug 10 19:21:40.773832 bgp_rcv_nlrri: 0.0.0.0/0 qualified bnp->ribact 0x0
12afcb 0x0
```

7. Pause the **monitor** command by pressing Esc-Q.
To unpause the output, press Esc-Q again.
8. Halt the **monitor** command by pressing Enter and typing **monitor stop**.

```
[Enter]
user@host> monitor stop
```

9. When you are finished troubleshooting, consider deactivating trace logging to avoid any unnecessary impact to system resources.

```
[edit protocols bgp group internal-peers]
user@host:A# deactivate traceoptions
user@host:A# commit
```

When configuration is deactivated, it appears in the configuration with the **inactive** tag. To reactivate trace operations, use the **activate** configuration-mode statement.

```
[edit protocols bgp group internal-peers]
user@host:A# show

type internal;
inactive: traceoptions {
    file bgp-log size 10k files 2;
    flag update detail;
    flag all;
}
local-address 192.168.6.5;
export send-direct;
neighbor 192.163.6.4;
neighbor 192.168.40.4;
```

10. To reactivate trace operations, use the **activate** configuration-mode statement.

```
[edit protocols bgp group internal-peers]
user@host:A# activate traceoptions
user@host:A# commit
```

Deactivating and Reactivating Trace Logging

Step-by-Step Procedure

To deactivate and reactivate the trace file:

1. When you are finished troubleshooting, consider deactivating trace logging to avoid an unnecessary impact to system resources.

```
[edit protocols bgp group internal-peers]
user@host:A# deactivate traceoptions
user@host:A# commit
```

When configuration is deactivated, the statement appears in the configuration with the **inactive** tag.

```
[edit protocols bgp group internal-peers]
user@host:A# show

type internal;
inactive: traceoptions {
    file bgp-log size 10k files 2;
    flag update detail;
    flag all;
}
local-address 192.168.6.5;
export send-direct;
neighbor 192.163.6.4;
neighbor 192.168.40.4;
```

2. To reactivate logging, use the **activate** configuration-mode statement.

```
[edit protocols bgp group internal-peers]
user@host:A# activate traceoptions
user@host:A# commit
```

Results

From configuration mode, confirm your configuration by entering the **show logical-systems A protocols bgp group internal-peers** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show logical-systems A protocols bgp group internal-peers
traceoptions {
  file bgp-log size 10k files 2;
  flag update detail;
}
```

Verification

Confirm that the configuration is working properly.

Verifying That the Trace Log File Is Operating

Purpose Make sure that events are being written to the log file.

Action user@host:A> **show log bgp-log**
Aug 12 11:20:57 trace_on: Tracing to "/var/log/A/bgp-log" started

Example: Configuring System Logging on Logical Systems

This example shows how to configure system logging on logical systems and how to view the logs.

- [Requirements on page 166](#)
- [Overview on page 167](#)
- [Configuration on page 167](#)
- [Verification on page 168](#)

Requirements

This example has the following requirements:

- You must have the **view** privilege for the logical system.
- Junos OS Release 11.4 or later.

Overview

Each logical system has its individual directory structure created in the `/var/logical-systems/logical-system-name` directory. This directory contains the following subdirectories:

- `/config`—Contains the active configuration specific to the logical system.
- `/log`—Contains system log and tracing files specific to the logical system.

To maintain backward compatibility for the log files with previous versions of Junos OS, a symbolic link (symlink) from the `/var/log/logical-system-name` directory to the `/var/logical-systems/logical-system-name` directory is created when a logical system is configured.

- `/tmp`—Contains temporary files specific to the logical system.

The file system for each logical system enables logical system users to view trace logs and modify logical system files. Logical system administrators have full access to view and modify all files specific to the logical system.

Logical system users and administrators can save and load configuration files at the logical system level using the **save** and **load** configuration mode commands. In addition, they can issue the **show log**, **monitor**, and **file** operational mode commands at the logical system level.

This example shows how to configure system logging on a logical system.

Configuration

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.

```
set logical-systems lsys1 system syslog host 10.209.10.69 ftp critical
set logical-systems lsys1 system syslog allow-duplicates
set logical-systems lsys1 system syslog file lsys1-file1 daemon error
set logical-systems lsys1 system syslog file lsys1-file1 firewall critical
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure system logging:

1. Configure trace operations on the logical system.

```
[edit logical-systems lsys1 system syslog]
user@host# set host 10.209.10.69 ftp critical
user@host# set allow-duplicates
user@host# set file lsys1-file1 daemon error
user@host# set file lsys1-file1 firewall critical
```

2. If you are done configuring the device, commit the configuration.

```
[edit]
user@host# commit
user@host# exit
```

Results

From configuration mode, confirm your configuration by entering the **show logical-systems** command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
user@host# show logical-systems
lsys1 {
  system {
    syslog {
      host 10.209.10.69 {
        ftp critical;
      }
      allow-duplicates;
      file lsys1-file1 {
        daemon error;
        firewall critical;
      }
    }
  }
}
```

Verification

Confirm that the configuration is working properly.

Verifying That the System Log File Is Operating

Purpose Make sure that events are being written to the log file.

Action



TIP: To make entries in the system log, you can use the **start shell** command and then use the **logger** shell command. For example: **logger -e "firewall_crit" -p firewall.crit -l lsys1 TEST**

```
user@host> show log lsys1/lsys1-file1
Sep 7 14:15:46 host clear-log[2752]: logfile cleared
Sep 7 14:19:04 host logger: % -: firewall_crit: TEST
...
```

```
user@host> file show /var/logical-systems/lsys1/log/lsys1-file1
Sep 7 14:19:04 host logger: % -: firewall_crit: TEST
...
```

Related Documentation

- [Introduction to Logical Systems](#)